



Expert Roundup:

# Is Internet Security a Losing Battle?



# Intro

A while ago, one of our readers asked us to answer the following questions:

*“Is Internet security a losing battle? How come companies are always 1-2 steps behind the fight? How can the bad guys respond so fast?”*

That reader is certainly not the only one with this issue on his mind. Many Internet users feel discouraged by the current state of cybercrime and its consequences, and the rest don't yet understand why they should care about it. We wanted to do something to change this.

**Naturally, users like you and me are not the only ones who wrestle this dilemma.** Within the industry, cyber security experts are deeply involved in studying the causes and changes which have brought us to this point so they can create better solutions. Each

of these experts brings a different perspective to the discussion, because no single person can ever claim to have the full picture.

That is why we reached out to some of the most experienced cyber security specialists in the field to gather their thoughts on the topic. We believe that the questions we received are justified and they deserve an honest answer. And you will find plenty of them below!

These answers will help clarify some of the challenges we're facing and I believe they'll also inspire you to act for your own online protection. You'll find a "**Read full text**" link on some of them – don't hesitate to click on it to read their entire contribution. What's more, we plan to keep this roundup open, so if you want to contribute, I would be thrilled to **hear from you!**

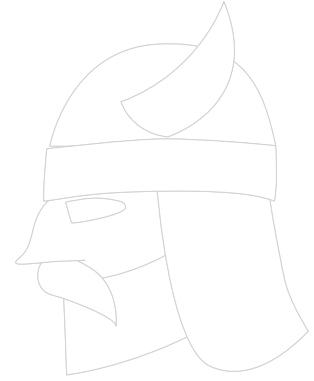
Here's a quick list of links that point to all the answers in the roundup, if you need to find them faster:

1.	<b>Alexandre Campos - IT Security Professional</b>	Pag. 1
2.	<b>Alexandru Stoian - CERT-RO</b>	Pag. 3
3.	<b>Andrei Avădănei - Bit Sentinel, DefCamp</b>	Pag. 7
4.	<b>Andrei Petruș - Avira</b>	Pag. 11
5.	<b>Andy Patel - F-Secure</b>	Pag. 15
6.	<b>Arosha K. Bandara - The Open University</b>	Pag. 17
7.	<b>Brian Beyst - MyAppSecurity</b>	Pag. 23
8.	<b>Brian Donohue - Cyber4Sight</b>	Pag. 27
9.	<b>Claus Houmann - Peerlyst</b>	Pag. 30
10.	<b>Cody Jackson - Inflow NS</b>	Pag. 33
11.	<b>Dave Piscitello - Geneva Centre for Security Policy, ICANN</b>	Pag. 35
12.	<b>David Bisson - Tripwire</b>	Pag. 39
13.	<b>David Harley - ESET</b>	Pag. 43
14.	<b>David Strom - Security Evangelist</b>	Pag. 54
15.	<b>Inbar Raz - PerimeterX Inc.</b>	Pag. 60
16.	<b>Jeff M. Spivey - ISACA, Security Risk Management, Inc.</b>	Pag. 75
17.	<b>Joaquín Pérez Ruiz - IT Control &amp; Risk Manager</b>	Pag. 78

18.	<b>Kevin Townsend - Cyber Security Journalist</b>	Pag. 83
19.	<b>Lawrence Abrams - Bleeping Computer</b>	Pag. 87
20.	<b>Liviu Arsene - Bitdefender</b>	Pag. 92
21.	<b>Mădălin Dogaru - Sentientchip</b>	Pag. 94
22.	<b>Matthew Rosenquist - Intel Corporation</b>	Pag. 103
23.	<b>Morten Kjaersgaard - Heimdal Security</b>	Pag. 125
24.	<b>Neil Kemp - Network &amp; Security Limited</b>	Pag. 130
25.	<b>Pavel Krčma - Sticky Password</b>	Pag. 135
26.	<b>Peter Kruse - CSIS Security Group</b>	Pag. 137
27.	<b>Pierluigi Paganini - Bit4Id, ENISA, Security Affairs</b>	Pag. 141
28.	<b>Raul Popa - TypingDNA</b>	Pag. 143
29.	<b>Ryan J. Corey - Cybrary</b>	Pag. 148
30.	<b>Sergiu Sechel - EY IT Advisory Services</b>	Pag. 150
31.	<b>Stan Hanks - Columbia Ventures Corp</b>	Pag. 157
32.	<b>Ștefan Tănase - Kaspersky Lab Global Research &amp; Analysis Team</b>	Pag. 164
33.	<b>Tony Perez - Sucuri Security</b>	Pag. 167

33 Cyber Security Experts Weigh in on the question:

# Is Internet security a losing battle?



# Alexandre Campos

PROFESSOR, SOFTWARE DEVELOPER AND IT SECURITY PROFESSIONAL **Quora**



**Absolutely not.** But it's a hard battle that will never have an end since new means of attack are always emerging and within new technologies, there will be new vulnerabilities to be fixed.

The point is:

- Companies should understand how important is to keep a Security Team inside only to watch and teach their employees on how to change their own behaviors to improve security;
- Technology users (any technology user) should have in mind that they are the weakest part of this chain; if user fails, it could lead to a security lack and this is not fantasy as we've seen in Hollywood, this is



# Alexandre Campos

PROFESSOR, SOFTWARE DEVELOPER AND IT SECURITY PROFESSIONAL [Quora](#)



real (it's not easy to convince the average user of some security practices, but it has to change);

- Costs are not low and if the company does not have enough financial resources to fix or reduce all its risks to a very low level, that it at least put them under an acceptable level, which it's better than nothing.



# Alexandru Stoian



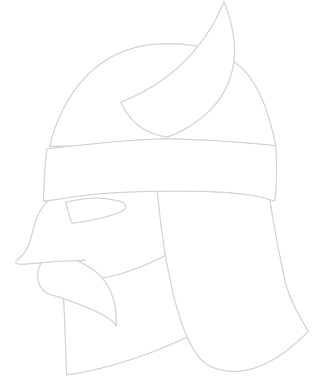
SECURITY CONSULTANT & DEVELOPER AT CERT-RO



The question you asked has a relatively simple answer. **The challenge is changing the public's perception towards it.**

Consequently, the battle against the Internet's "insecurity" is similar to many other daily battles that people are involved in. One can also fight against classic crimes or any other activity that implies a certain amount of "maintenance" and I don't think the problem is exhaustible or solvable. If you wish, this is a chronic disease.

For any company that's involved in the cyber security industry, the goal is not to eliminate these insecurities (an impossible goal). The purpose is to mitigate their effects and acknowledge the threat.



# Alexandru Stoian

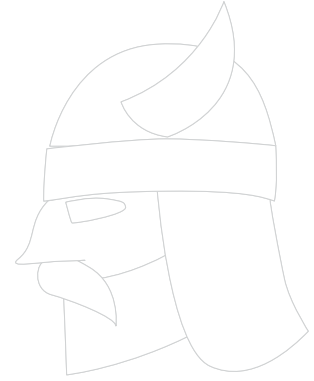
SECURITY CONSULTANT & DEVELOPER AT CERT-RO



In the beginning (the '00s), cyber security wasn't something to invest a lot of time or money into. For malicious actors, the opportunities to make money were numerous, but modest when it came to return on investment. You didn't need deep technical knowledge to access personal data or financial information.

However, nowadays, the ability to exploit vulnerabilities has been reduced to personal websites or smaller organizations that don't have a significant online presence or too much to lose in the aftermath of a successful cyber attack.

In order to carry such an attack, one would need knowledge which is not easily accessible. Generally speaking, the latest attacks



# Alexandru Stoian

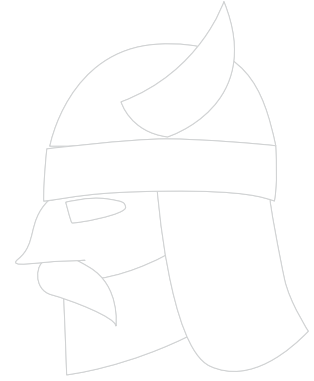
SECURITY CONSULTANT & DEVELOPER AT CERT-RO



(except for DDoS attacks) to catch the media's attention were caused by social engineering tactics, not necessarily by unprotected infrastructures. Also, the financial impact on the targeted company is also a lot bigger in these cases.

Even these attacks (that include a social engineering component) are more difficult to execute these days, especially because netizens and/or employees have already been immunized by seeing so many ransomware and spam campaigns and more. This is where the awareness part is more visible.

If you wish, the situation can be compared to another concept we frequently come across in game theory: the Red Queen Hypothesis. Such "races" are frequently seen in



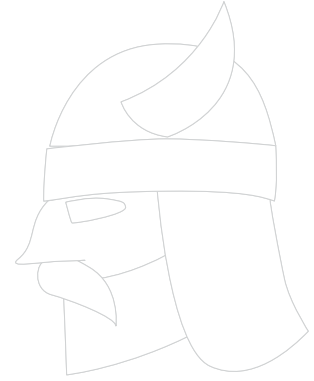
# Alexandru Stoian

SECURITY CONSULTANT & DEVELOPER AT CERT-RO



nature and as long as someone can take advantage of the lack of security, someone will do it. Also, as long as someone will try to stop malicious actors from exploiting these security holes, the bad guys will have to adapt and, occasionally, to lose.

So, the short answer to the question is: as long as we're fighting this battle and believe we can win it, we can't lose.



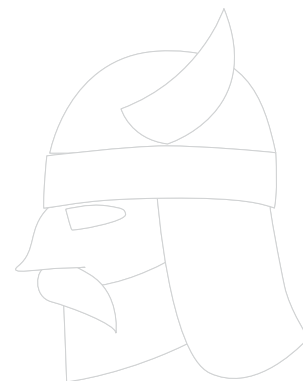
# Andrei Avădănei

CEO AT BIT SENTINEL, FOUNDER AT DEFCAMP



**Absolutely not.** But it's a never-ending story because of the emerging new technologies that will always have new vulnerabilities to be fixed. This happens mainly because of one reason – humans.

Humans develop technologies and sometimes there is management or a deadline pressure in order to deliver fast without proper care to security. There is also a lack of education – entities need to better understand the importance of security for their valuable assets. I believe that a good cyber security provider will always tend to minimize the risks and impact of security incidents and not completely remove the threats, so there is always room for a novel approach to attack the target. But this is really hard to explain for casual users or



# Andrei Avădănei

CEO AT BIT SENTINEL, FOUNDER AT DEFCAMP

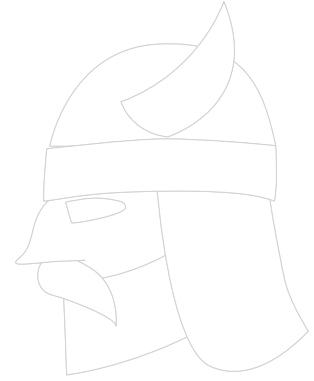


entities.

Also, adding new technologies, which are still built by humans, in the infrastructure (even security technologies) will sometimes bring new attack vectors in the network. Even machine learning and deep learning algorithms have their limitation and they are still developed by humans.

On the other side, cyber crime is a good-income business model and investing in their “business” core makes sense. They need to discover innovative ways to abuse companies and individuals’ wealth in order to keep up with new security solutions & approaches but also maintain the income coming.

Although we are at the end of 2016, we are



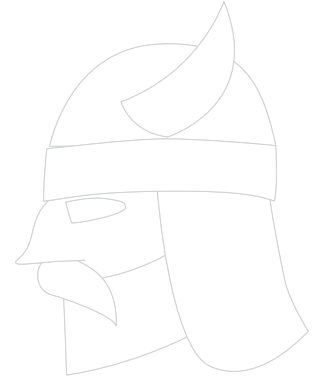
# Andrei Avădănei

CEO AT BIT SENTINEL, FOUNDER AT DEFCAMP



(and will) still relying on very old technologies and infrastructures. We hide time bombs on the newly added layers of abstraction and optimization which, at some point, will be discovered by the security researchers community or by the cyber crime teams.

On top of everything, each technology, device or infrastructure still relies on humans. And we fail because we think “it’s not gonna happen to me”. Social engineering attacks tend to get better at using real information about our personal or work life. And, when nowadays with just a click millions can disappear, raising awareness among the employees it’s a must do in any company.



# Andrei Avădănei

CEO AT BIT SENTINEL, FOUNDER AT DEFCAMP

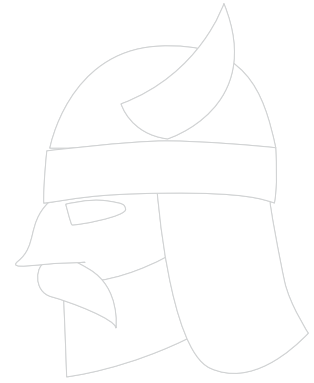


But, on the good side of the story, with each new vulnerability, the cyber security community tends to get better at protecting assets & identifying threats, making it harder and more expensive for the attackers to come up with something new.



# Andrei Petruș

PRODUCT MANAGER AT AVIRA

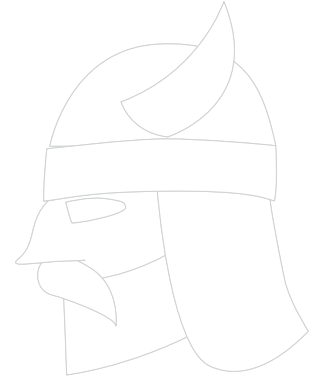


Maybe the question is wrong.

First, let's accept the Internet is a key enabler that took us on the exponentials of digitization, responsible for the oh-so-many innovations that transformed our lives for the better – making us more connected and efficient.

Second, we need to understand that progress is built on our capacity to adopt and galvanize innovation, which is nothing but a function of counterbalancing risk with benefits.

**Now we are prepared to ask it the right way: "If it wasn't for the internet security industry, how would the present look like?". Putting on the immersion lens we can do a branch-**



# Andrei Petruș

PRODUCT MANAGER AT AVIRA



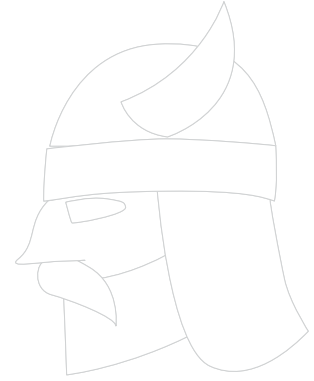
ing here and see possible outcomes.

## Option A – Security over progress

Where there's money, crooks will follow and risk will accumulate. This stays true in the physical world, as well as in the digital realm. Just because of this, we could have put a stop to developing Internet products and services, in direct response to our fear that we are not able to protect them.

## Option B – Progress over security

Racing against opportunities is a hard one in the capitalist age. This is why we could have neglected security and privacy, to freely run an economy that yields a profit. Blindfolded, we would soon realize that ignoring security



# Andrei Petruș

PRODUCT MANAGER AT AVIRA

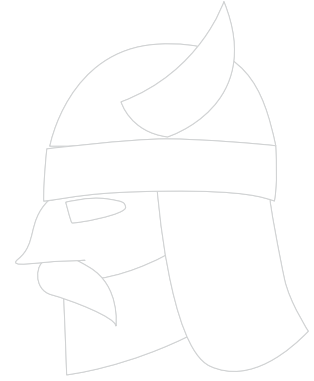


and privacy is going to collapse the whole system.

## Option C – Our future

Whilst both of the above options are dystopian, we've set the premises for a different future – the one we have laid ahead of us now, opening doors wide for technology advancements and building up the stepping stones for breakthroughs in areas such as bioengineering, space exploration, clean energy, advanced robotics, virtual reality, autonomous driving, shared economy, AI, to name a few.

At the same time, the information security industry put guardians at each of those doors to make sure integrity, privacy, and



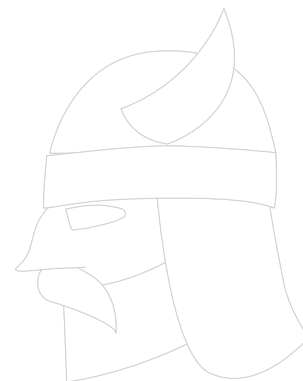
# Andrei Petruș

PRODUCT MANAGER AT AVIRA



resilience are enforced. We have now a strong portfolio of products and services that safeguard traditional layers of the Internet technology, as well as the now-exploding IoT and IIoT realms. Of course, there's no such thing as 100% protection, but each player in the infosec space puts a piece to the puzzle that maintains the **equilibrium between progress and security.**

# Andy Patel



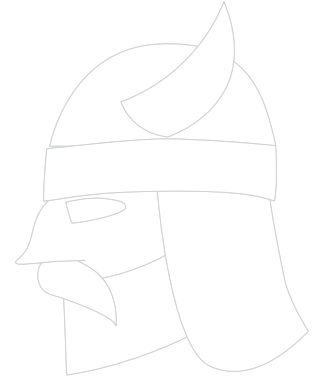
CYBER GANDALF AT F-SECURE



**No.** But that depends on what you mean by “The Internet.”

Ask the average individual “what is the Internet?” and you’ll likely get a range of answers including the web, apps, the cloud, IoT, and down the road, even stuff like AI chat bots. Not all of this stuff will exist in the future as it does now. Some of the change may be forced by security issues, and some for other reasons. The Internet will evolve.

Security will drive parts of this evolution – things that are harder to secure will change or die off faster than they might have otherwise. It might be a losing battle to defend something that is mostly dead just for the sake of fixing security issues. There’s also the fact that there are a bunch of different

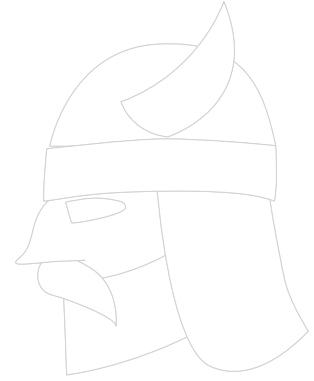


# Andy Patel

CYBER GANDALF AT F-SECURE



“Internets” emerging. Russia and China have their own versions of services that others use. Internet balkanization may continue to occur into the future. And all of those separate Internets will have their own security issues to deal with. **It’s not a losing fight, but choose your battles wisely.**



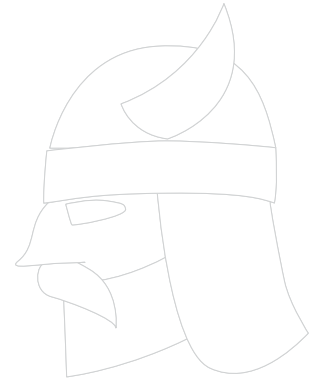
# Dr. Arosha K. Bandara

SENIOR LECTURER IN COMPUTING AT THE OPEN UNIVERSITY



It is now common to see a deluge of news stories reporting on a range of successful cyber security attacks, from internet connected appliances being used to launch denial of service attacks (<http://www.bbc.co.uk/news/technology-37738823>), to the unauthorized access to personal data by hacking into online service providers' systems (<http://www.zdnet.com/article/daily-motion-hack-exposes-millions-of-accounts/>).

From this, it seems obvious to conclude that the attackers are winning and the only safe course of action is to stop using internet connected technologies. However, jumping to such a conclusion ignores the less reported successes in thwarting attacks that happen every day. This includes the globally



# Dr. Arosha K. Bandara

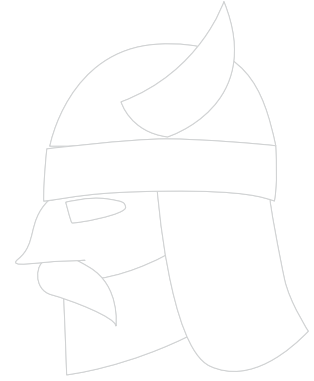
SENIOR LECTURER IN COMPUTING AT THE OPEN UNIVERSITY



coordinated actions against cybercriminals (<https://www.fbi.gov/news/stories/joint-cyber-operation-takes-down-avalanche-criminal-network>), as well as the actions of systems administrators and dev-ops specialists to keep their systems secured from attack. It also undervalues the advances in technology and processes, as well as the growth in knowledge and skills that have been developed to better protect Internet-connected systems.

In the words of Bruce Schneier, “**Security is a process, not a product**”, and in this spirit, we should recognize that internet security isn’t a battle **that can be concluded with a decisive win or loss but rather an ongoing activity that we are all engaged in**. Indeed, in this context, the metaphors of conflict, such





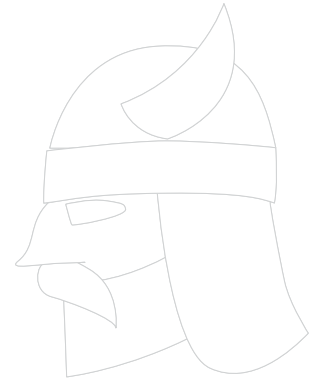
# Dr. Arosha K. Bandara

SENIOR LECTURER IN COMPUTING AT THE OPEN UNIVERSITY



as 'war' and 'battle' are unhelpful because they suggest that internet security is the responsibility of the technologists who act our defensive force against attackers.

Instead, as has been argued by technology activists like Cory Doctorow (<https://www.theguardian.com/technology/2014/mar/11/gchq-national-security-technology>) and others (<http://dtdc.webscience.ecs.soton.ac.uk/wp-content/uploads/A-Public-Health-Approach-to-Cybersecurity-by-Huw-Fryer.pdf>), we might have more success by thinking of cyber security using the analogy of public health and communicable diseases. By using this analogy, we make cyber security issues more relevant to people and spur them to gain a



# Dr. Arosha K. Bandara

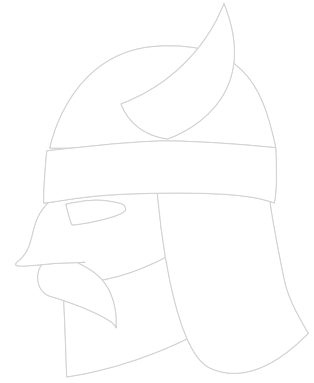
SENIOR LECTURER IN COMPUTING AT THE OPEN UNIVERSITY



better understanding that, like diseases, any of us can be afflicted by a cyber security attack.

**We can also adopt an analogous approach for handling cyber security threats, through a process of education and management** (e.g., making people aware of how their home network hub could be compromised due to not changing the factory default password); **prevention** (e.g., designing hubs to require users to change the default passwords on installation and update firmware before connecting to the Internet) and **management** (e.g., disabling the Internet connection of a hub if it is configured with default passwords or out of date firmware).

We are starting to see this shift in approach



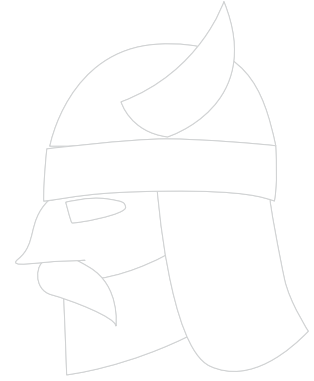
# Dr. Arosha K. Bandara

SENIOR LECTURER IN COMPUTING AT THE OPEN UNIVERSITY



through **accessible educational content**, such as The Open University's Introduction to Cyber Security MOOC (<https://www.futurelearn.com/courses/introduction-to-cyber-security>) and the UK Government's Cyber Aware campaign (<https://www.cyber-aware.gov.uk>). **This needs to be linked to a holistic approach that ties this broader awareness of cyber security to giving everyone access to effective tools for prevention and management.**

If we do this, **I don't think that Internet security is a losing battle.** Instead, it becomes an ongoing process of awareness, investigation, and innovation to detect, diagnose and treat a global epidemic that affects us all. Then, just as we have managed numerous global public health challenges, we will be



# Dr. Arosha K. Bandara

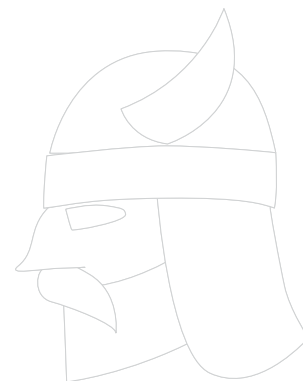
SENIOR LECTURER IN COMPUTING AT THE OPEN UNIVERSITY



able to manage the security of our digital lives.

# Brian Beyst

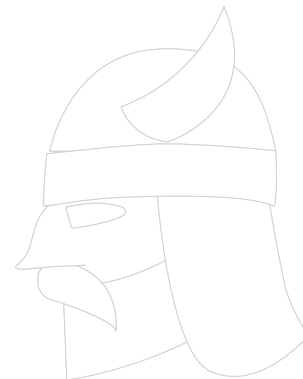
SENIOR DIRECTOR OF MARKETING AT MYAPPSECURITY



From a defense-oriented security posture, yes, it is a losing battle. Such a posture is like a blindfolded person playing whack-a-mole – while **patches** are being applied to one area on the comprehensive **attack** surface, the bad guys just show up in another area.

**The key to getting ahead of the attackers requires being proactive in three key areas:**

1. Understanding the **risks** and **threats** inherent in the **applications** and the infrastructure (which are two separate issues);
2. Understanding the means, motive, and opportunities of the attackers – this is significantly more challenging than just labeling an **attacker** with a **profile** name, it involves understanding what the attackers are after



# Brian Beyst

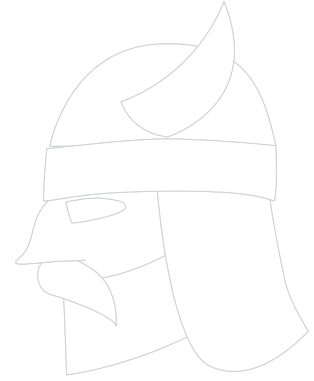
SENIOR DIRECTOR OF MARKETING AT MYAPPSECURITY



and what they bring to the attack to help them be successful; and

3. Understanding what it is you're trying to protect – the **information assets** and **system** capabilities which can be reached through the applications and IT system.

Understanding these three areas allows security to prioritize their defenses and proactively shore up the security weaknesses before they become exploited vulnerabilities. This can only be achieved through a matured **threat modeling process** that scales across the entire **DevOps** portfolio. When **threat** modeling is used to prioritize cyber security, the limited available **resources** may be properly prioritized and proactively applied.



# Brian Beyst

SENIOR DIRECTOR OF MARKETING AT MYAPPSECURITY

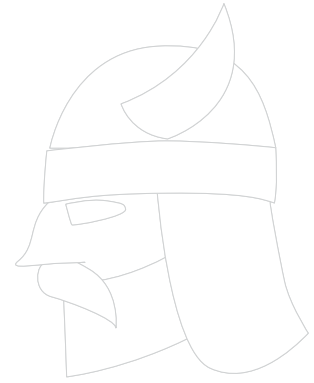


THEN **Internet Security** may become a winning battle, making it increasingly difficult and expensive for attackers to find and **exploit vulnerabilities** that satisfy their goals.

**Is Internet security a losing battle?** Find out from these 30+ #cybersecurity experts:







# Brian Donohue

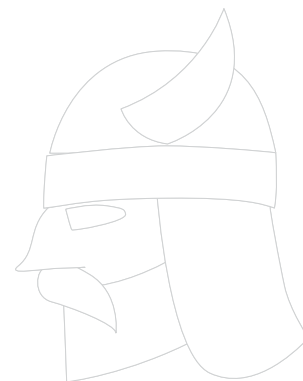
JOURNALIST AND THREAT INTELLIGENCE ANALYST AT CYBER4SIGHT



## If Internet Security is a Losing Battle, Then We Should All Just Quit

Simply put, if we're going to have a constructive conversation about what's wrong with Internet security, then we simply can't call it a losing battle. The sanest response to a struggle that will inevitably end in failure is to give up. It's simple math, really: *why waste resources trying to generate an outcome that won't ever materialize?* If the cost of continuing the fight is greater than the costs associated with giving it up and ultimately losing, then you quit. It's a no-brainer—albeit one that history can prove is often ignored.

However, with Internet security, the equation becomes more complicated. First and foremost, **we aren't fighting one clear battle, but**



# Brian Donohue

JOURNALIST AND THREAT INTELLIGENCE ANALYST AT [CYBER4SIGHT](#)



**a war consisting of many millions of battles, concealed in a dense fog, against largely unknowable enemies.** Despite this, the defenders may be winning. While the media is awash with stories of devastating cyber attacks, by and large, the integrity of online transactions and communications is intact. Spam may outstrip legitimate email traffic, but spam filters effectively mean that few people experience the spam. Distributed denials of service and Internet of Things botnets may be the talk of the town, but, in the end, most Web traffic is legitimate. Ultimately, if we could somehow quantify the legitimate and compare it to the malicious on a grand scale, I am confident that the legitimate would carry greater numbers.

That said, there is a very real appearance of

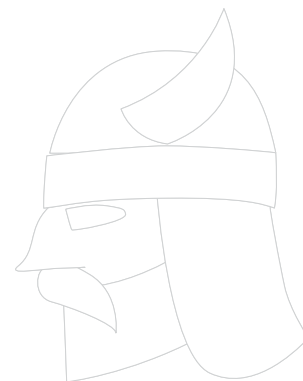


# Brian Donohue

JOURNALIST AND THREAT INTELLIGENCE ANALYST AT [CYBER4SIGHT](#)



losing, but think about how much worse the actual losses would be if we all just threw up our hands, tore down the firewalls, and walked away. So no, **Internet security is not a losing battle; it's a perpetual war that we'll never win outright.** Even as security technologies get better, new attack techniques proliferate. Essentially every defensive breakthrough is offset by an offensive one. It may be the case that no matter how good we get at security, so to speak, the success rate for the attackers will never decrease and, likewise, that of the defenders will never meaningfully increase. That doesn't mean the battle or the war is lost; it just means that **we have to learn to accept a certain level of failure in a fight that is totally worth fighting.**



# Claus Houmann

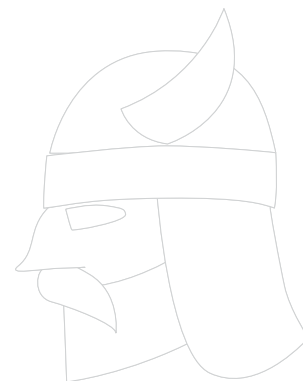
COMMUNITY MANAGER AT PEERLYST



The DHS Secretary Johnson yesterday said, “Growing dependency on network-connected technologies is outpacing the means to secure them.”, which is very similar to the quote by IATC founder Josh Corman, which Josh has been repeating for years – that **our dependence on technology is increasing faster than our ability to secure it.**

*Is Internet security a losing battle?, you ask, and my answer will be this:*

In the history of mankind, our species have faced several huge challenges and times of trouble. Never ever have we given up fighting a battle. The battle that is securing the Internet is a battle that we have never fought before, we have no experience and no reliable tactics so we will inevitably make mis-



# Claus Houmann

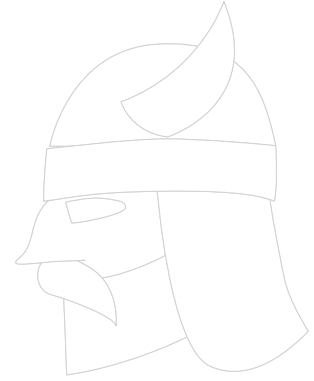
COMMUNITY MANAGER AT PEERLYST



takes, but I believe that by the same methods that we solved challenges like plague-like diseases, which were solved by successive individual contributions similar to so many other solutions, we will eventually find ways that will raise the bar for Internet security significantly.

This means that **I believe that we all must try to do our part** and that each individual effort added to this collective effort has a payoff, and that when enough of us unite our voices and our efforts, it will have an impact and things will get better.

So, in my opinion, those sitting on their couches with the phones tweeting “Security thing X is broken” or “Infosec is broken, totally” – they are not helping. **We need to**



# Claus Houmann

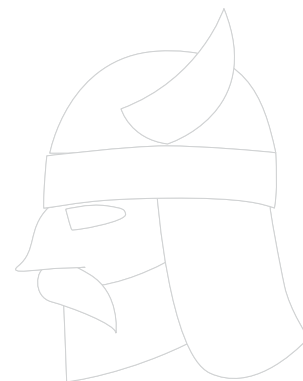
COMMUNITY MANAGER AT PEERLYST



**DO this together**, try to things better together and stop sitting on our 400lb hacker behinds (famous Trump quote) and complaining. If enough people try to make a difference, then either someone will successfully do so, or eventually the combined voices of those trying will turn the tide.

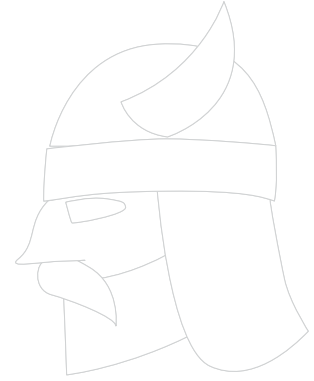
# Cody Jackson

SOFTWARE DESIGN ENGINEER AT [INFLOW NS](#) [Quora](#) [in](#)




In general, no. **If you don't keep up your defenses, then you have lost the battle.** While it may cost a lot in time and money to maintain your defenses, at least you have a chance, because every time a new attack vector is found, a defense is created for it. It's not a question of "if" you've been hacked, it's a question of "when".

On the flip side, however, because a lot of organizations don't take security seriously, they leave themselves and others open for attack. Whether it's retailers that don't bother to encrypt their databases or IoT and auto manufacturers who want to be first to market, rather than taking the time to build with security, they are making the Internet less safe for everyone else.



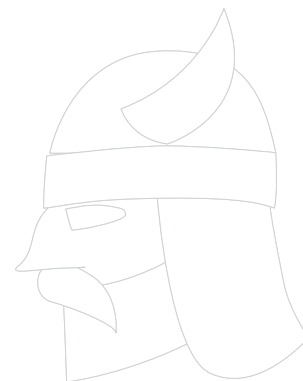
# Cody Jackson

SOFTWARE DESIGN ENGINEER AT [INFLOW NS](#) [Quora](#) [in](#)



So, **it will be a never-ending battle**, at least until a new Internet design is developed that has security built-in but, even then, security researchers will still be able to stay in business.





# Dave Piscitello

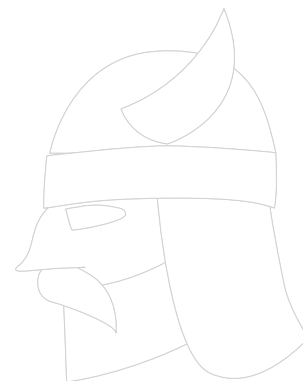
ASSOCIATE FELLOW AT [GENEVA CENTRE FOR SECURITY POLICY](#),  
VP SECURITY AND ICT COORDINATION AT [ICANN](#)



Any battle that you engage on your enemy's terms, with indefensible assets or limited offensive capabilities, and where your enemy's risk and cost of attack is small is arguably a losing battle.

However, I'm not certain that warfare remains the right analog for Internet security today. I think that health may be a better analog. Here's why:

- **The devices and software that comprise the Internet are organisms that are not perfectly healthy from the moment they're installed.**
- **Their immune systems are weak** (e.g., poorly designed, lacking secure code review...) and further weakened by poor hy-



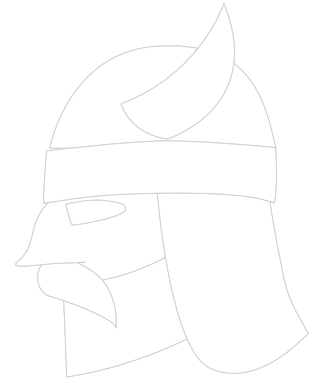
# Dave Piscitello

ASSOCIATE FELLOW AT GENEVA CENTRE FOR SECURITY POLICY,  
VP SECURITY AND ICT COORDINATION AT ICANN



giene (e.g., lax administration, default configuration).

- **They are premature**, we know it, and we persist in imagining that persistent incubation or health monitoring and triage (secure perimeters, firewalls, IDS/IPS) would suffice. Moreover, these systems are themselves fragile: the same hardware, software, or administrative fragility exists among these systems.
- **The people who use devices and software are largely not care providers nor did they expect to be when they acquired devices.** They are in large part ignorant or in denial of this fragility and the very real threat these pose to their own health (financial harm, loss of privacy, etc.). They are also



# Dave Piscitello

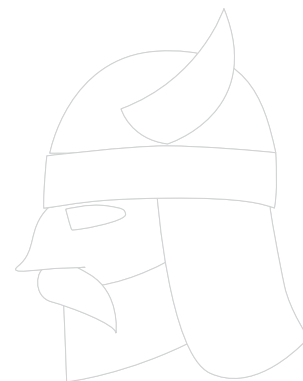
ASSOCIATE FELLOW AT [GENEVA CENTRE FOR SECURITY POLICY](#),  
VP SECURITY AND ICT COORDINATION AT [ICANN](#)



addicted to the extent that they would not sacrifice the advantages the Internet offers, perhaps irrespective of the degree of risk.

**The biggest challenge with Internet health is that the organisms change at a faster rate than the human body.** New Internet organisms appear hourly (apps, networks, IoT devices). There are common DNA or genomes among these, but that is in fact part of the problem! We re-use or adapt what is problematically unhealthy in each generation of new organisms. We are effectively nurturing an unhealthy ecosystem and in tandem, nurturing an Internet that is very negatively affected by infectious disease.

**I think we'd need to pause, thoughtfully design "healthy" devices or software. We**



# Dave Piscitello

ASSOCIATE FELLOW AT [GENEVA CENTRE FOR SECURITY POLICY](#),  
VP SECURITY AND ICT COORDINATION AT [ICANN](#)



need easily understood and easy to adopt immunization and hygiene protocols. This is hard work. Expensive work. It flies in the face of conventional Internet drivers. It's more likely that we'll continue along the conventional path until some apocalyptic event forces change.

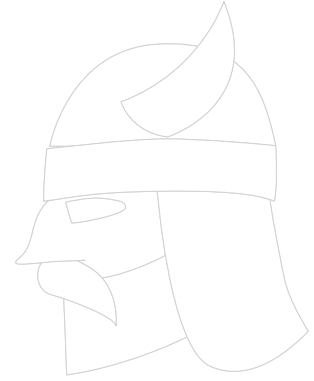
# David Bisson

ASSOCIATE EDITOR AT TRIPWIRE



**Internet security is a losing battle only if you look at security in absolute terms.** In this frame of mind, you're either secure against every type of online threat, or you're completely exposed. As we all know, Internet security doesn't work that way. It's not a static binary; it's a process. Part of that process involves learning about new threats and working through effective mitigation strategies.

Now, sometimes the proliferation of threats might seem a bit overwhelming. *How could it not?* But not everything's doom and gloom. After all, most attacks aren't reinventing the wheel. They're reusing what's been working for years if not decades. Some campaigns pass malicious links to unsuspecting users, while others exploit vulnerabilities to gain



# David Bisson

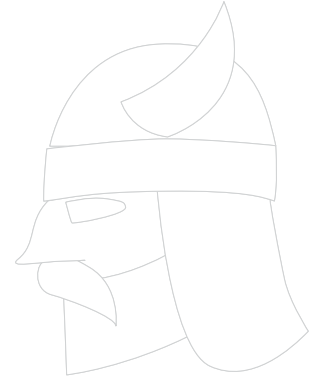
ASSOCIATE EDITOR AT TRIPWIRE



access to an organization's network. Today's malware might come with new capabilities, but many of the attack vectors are the same.

In this light, **Internet security is all about understanding how you can best leverage your people, processes, and technology to uphold the security basics.** For instance, organizations can use security awareness training software (technology) as a means to promote ongoing anti-phishing education (process) among its workforce (people). They can also create a vulnerability management program under which endpoint detection and response solutions actively scan network nodes for known vulnerabilities and for suspicious behavior.

**It's impossible to stay on top of ALL threats.**



# David Bisson

ASSOCIATE EDITOR AT TRIPWIRE

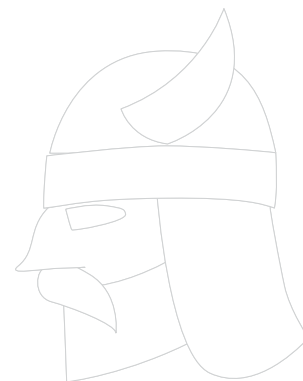


**But as long as we continue to think, adapt,  
and learn, Internet security will never be a  
losing battle.**

**Can you win the fight against  
#cybercriminals?** See what 30+  
cyber security specialists think:







# David Harley

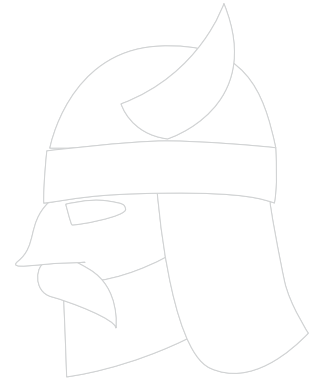
SENIOR RESEARCH FELLOW AT ESET



It depends on what you expect to be achieved, in terms of security. We're not going to be able to put a stop to all cyber-crime and malicious activity online, any more than the medical profession is going to be able to eradicate disease, or law enforcement agencies have been able to eradicate "real world" crime.

**Internet security is an attempt to solve a number of social problems**, and at the moment the solutions we have are mostly technological rather than social.

The security industry is pretty good at providing a wide range of partial solutions to a wide range of technological attacks, but technology continuously evolves on both sides of the white-hat/black-hat divide, so –



# David Harley

SENIOR RESEARCH FELLOW AT ESET



marketing claims notwithstanding – there is never 100 percent security across the board. Least of all from a single product. In fact, the very question to which I’m responding echoes a widespread feeling that ‘Since the security problem can’t be solved, there is no point in trying to solve it.’

However, using a variety of well-chosen security products and services – we sometimes call this multi-layering – can reduce the risks very significantly. For a business, that might mean a ‘moat and wall’ assembly of multiple defensive technologies at the perimeter and inside the organization, with a trained team to administer it. But only the most paranoid individuals will have the necessary knowledge (or even desire) to set up a comparable range of defenses. **Fortunate-**



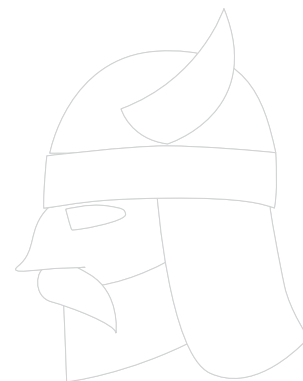
# David Harley

SENIOR RESEARCH FELLOW AT ESET



**ly, it is possible for individuals to defend their systems reasonably effectively without directly evaluating and implementing a wide range of defensive programs:** for example, by installing security suites that combine the functionalities of a range of technologies. (For instance anti-malware, personal firewall, anti-spam and so on.)

However, even multi-layered technological solutions cannot be assumed to provide that 100 percent security we'd all want to achieve if we could. In part, this is because both malicious and defensive technologies are constantly in a state of tension: sometimes a breakthrough from one side or the other will put that side well ahead, but in due course, the other side will catch up, or even make an equally dramatic breakthrough. Often,



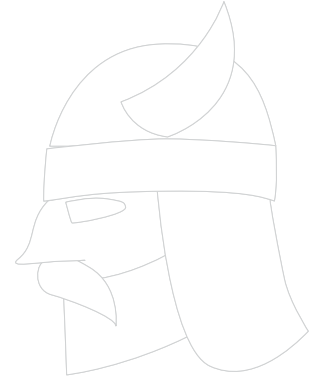
# David Harley

SENIOR RESEARCH FELLOW AT ESET



whether a threat is automatically detected or blocked is as much a matter of good or bad timing as it is of the technical effectiveness of the threat. **Very, very often, though, a threat is less dependent on the effectiveness of its technology than it is on how effectively it manipulates the psychology of the victim.**

Psychological manipulation of the intended victim is a core component of what we often call social engineering. **Susceptibility to social engineering** can sometimes be reduced by technical measures – the textual analysis of email messages with the aim of detecting text that is characteristic of a certain type of criminally-motivated communication, for example. However, educationalists favor a complementary, longer-term



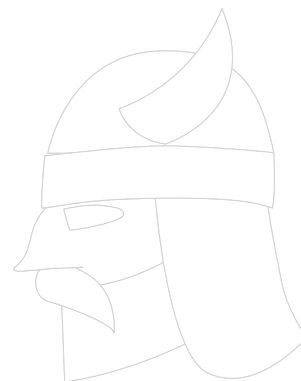
# David Harley

SENIOR RESEARCH FELLOW AT ESET



approach that involves making individuals less easy to manipulate. One step towards achieving this is through relatively simplistic training in threat recognition: for example, the 'phishing quizzes' that Andrew Lee and I looked at in 2007 in a Virus Bulletin paper (**[Phish Phodder: is User Education Helping or Hindering?](#)**).

Even a poorly designed quiz raises awareness of the problem but may be worse than useless if it reinforces wrong assumptions on the part of the quiz participant. Some quizzes seem to promote a service: 'Discrimination is too difficult for your tiny brain; buy our product, or even use our free toolbar/site verification service/whatever'. That's not wrong in itself; a vendor is in the business of selling products or services. If the product



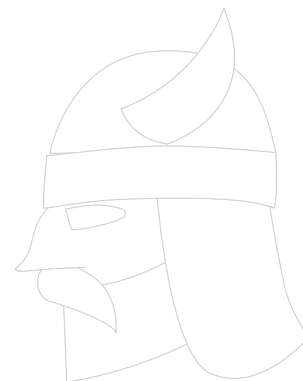
# David Harley

SENIOR RESEARCH FELLOW AT ESET



or service in question is free, it seems even more churlish to criticize, but there is a problem in that this message fosters dependence, not awareness; worse, that dependence is on a technical solution that is likely to rely on detecting specific instances of malice, rather than a generic class of detection.

Clearly there are limitations in the effectiveness of this approach. By showing potential victims a few example threats, it may sometimes be that they'll be able to extrapolate from those when faced with different examples in the same class. But not often enough. Yet, however desirable it might be in theory to provide everyone with the analytical skills of an effective security expert that clearly isn't a realistic possibility in the work-



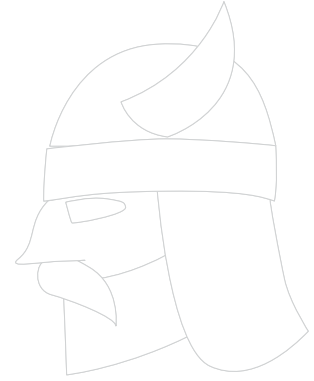
# David Harley

SENIOR RESEARCH FELLOW AT ESET



place, let alone at home.

**A better long-term solution might be to improve recognition of threats more generically through the teaching of critical thinking and the encouragement of skepticism.** Critical thinking has always been considered informally to be one of the principle aims of education, especially in academic centers for higher learning, and in recent years has been seen more often as a formal subject. For example Theory of Knowledge is a mandatory component of the International Baccalaureate. However, a review of Facebook posts and pages suggests that general education has so far been unable to make much of a dent in the general population's susceptibility to logical fallacy and cognitive bias.



# David Harley

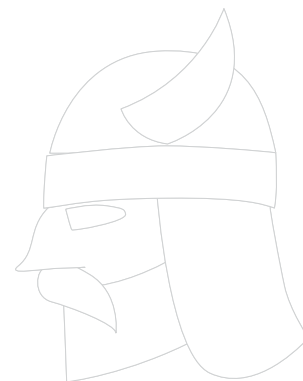
SENIOR RESEARCH FELLOW AT ESET



**Crime is an anti-social response to a range of factors:** societal, economic, political, cultural, and historical. It may sound to include society as a driver behind anti-social behavior, but it can certainly be argued that crime is to some extent built into a dystopian society (and most of us live in one of those). In other words, behaviors and attitudes are by no means always aligned with the religious, ethical and moral codes that are assumed to guide a society as a whole.

For example, individuals within societies that are generally regarded as Christian do not necessarily conform to the letter of the Ten Commandments or a literal reading of the Testaments. Recently, for example, we've seen an example of an election so highly-charged that suggestions of assassina-





# David Harley

SENIOR RESEARCH FELLOW AT ESET



tion have originated all along the spectrum from left to right. Hopefully, most of those suggestions were not serious attempts at incitement, but they do suggest a surprisingly thin veneer of adherence to the **Decalogue**.

**Anomie** has been defined (among many definitions!) as a condition where society provides insufficient moral guidance to the individual. However, it's entirely arguable that society can actually cause deviant behavior where the individual must subscribe to more than one code, yet elements of one code are incompatible with another, leading to an uncomfortable state of cognitive dissonance, which **might lead** to 'irrational or maladaptive behavior'. In other cases, perhaps it's just that in an era where fake news

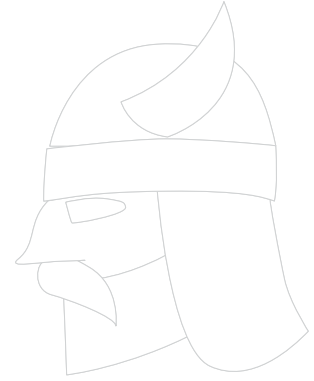
# David Harley

SENIOR RESEARCH FELLOW AT ESET



dressed up as satire is the common currency of the social media, the evolution of technology has far outstripped the average person's ability to apply the common precepts of everyday socialization to the online world.

**These problems are not going to be overcome by technology alone.** But in thousands of years, we've also failed, so far, to overcome the effects of criminality and the factors that underlie it – social and economic inequality, racial and religious intolerance, lust for power and money, diminishing resources, and empire building, for instance. If we have so much trouble re-engineering society into a less hostile environment, *can we at least reduce the impact of malicious behavior in the online world?* After all, 'Stop the Internet I want to get off' isn't an option



# David Harley

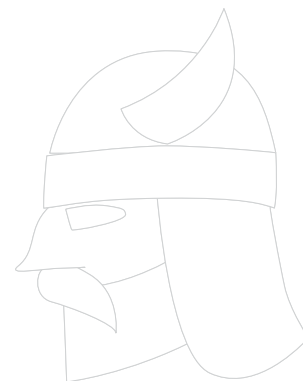
SENIOR RESEARCH FELLOW AT ESET



for most of us, still less for our children.

I was recently reminded of an [article](#) on Internet security, to which my main contribution was an argument that parents should regard themselves as educationalists and recognize that it is never too early to help their children to develop rational and critical thinking about what they see on the Internet and learn to trust their own judgment. It's part of a parent's responsibilities to learn enough about security and self-protection to share with their children. And part of that is to recognize just how unsafe the Internet is, not just as a vector for direct attacks, but also as a source of information.

# David Strom



EDITOR AT [INSIDE SECURITY](#), IT JOURNALIST,  
BUSINESS CONSULTANT, SECURITY EVANGELIST



I have been writing about Internet security for decades, and one of the things that I have seen is that making your home networks secure is NOT a losing battle. It is a *constant* battle, it is a difficult battle, it is sometimes a very frustrating and time-consuming and tiresome battle, but it is a **battle that can be fought and won**, if you take the time, have the tools, and understand the right techniques to fight it.

The key thought: **you need to fight this battle on the right fronts and be smart about it**. One place to start is right here on this blog. Take a look and review the suggestions in each of the following posts:

- [Ten steps to improve your wireless home networks](#)

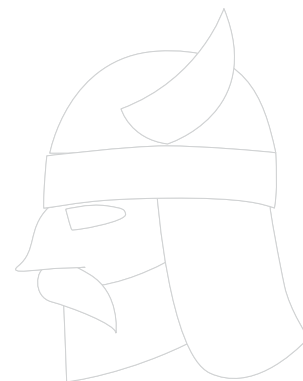
# David Strom

EDITOR AT **INSIDE SECURITY**, IT JOURNALIST,  
BUSINESS CONSULTANT, SECURITY EVANGELIST



- [Detecting phishing email campaigns through LinkedIn](#)
- [How to backup your devices](#)
- [Improve your privacy on LinkedIn and other social media accounts](#)
- [Recognize and avoid these common scams](#)
- [Strengthen and improve your passwords](#)

Taken together, this all may seem overwhelming and a lot of reading. It is. But use these articles as checklists to improve your cyber defenses. Most of the suggestions in these articles are relatively easy and quick



# David Strom

EDITOR AT **INSIDE SECURITY**, IT JOURNALIST,  
BUSINESS CONSULTANT, SECURITY EVANGELIST



solutions and can make your networks battle-ready a hundred or even a thousand times better. They don't cost much money, although they are time-consuming.

You need to do all of these actions: secure your wireless network, fight phishing, manage your passwords and backups. Really. **Better security is not a snack, it is a multiple-course meal.**

All it takes is one slip-up and your PCs can be invaded with a single phished email, an inadvertent click on a link that will download some malware, getting some infected message from Facebook or Skype, sharing a misdirected Tweet or some other mistake. That can be depressing, I agree. But it happens to all of us at some time.



# David Strom

EDITOR AT **INSIDE SECURITY**, IT JOURNALIST,  
BUSINESS CONSULTANT, SECURITY EVANGELIST



Here is one example: For the past 21 years, I have been sending out weekly emails to a mailing list. For years, I used a friend's basement computer to run as my list server. Then his basement flooded and his server was down for a few days until the waters receded. I was offline during this time, and I thought I was okay, except I realized one thing: the most crucial information, the email IDs of all my list recipients, **was never backed up**. Never. Thankfully, my friend took better care of my data than I did, and eventually, both he and I were up and running. Ever since then, I make a weekly backup of my list recipients. It doesn't take but a moment to send the right command to my list server to get this information.

Now I thought I had plenty of backups of my

# David Strom

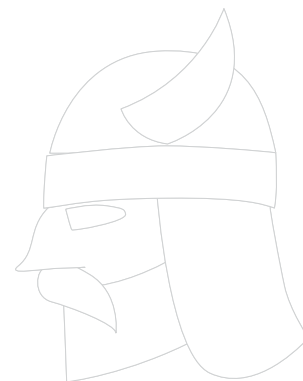
EDITOR AT **INSIDE SECURITY**, IT JOURNALIST,  
BUSINESS CONSULTANT, SECURITY EVANGELIST



office and home computers. But I was missing this one little thing. You can't be too careful, and luckily I was able to learn from the flooded basement and prevent a major business disaster.

So don't despair. You haven't lost the security war; you just have opened your eyes and hopefully can see what lies ahead. Given your reading assignments, you will do better the next time you might not open your virtual door to some criminal, or hesitate when you need to reply to someone who is masquerading as your friend or avoid some other tactical error. Just because your PC got compromised recently doesn't mean you should give up, unless you plan on living on some remote island without any Internet access or computers for the rest of your life.





# David Strom

EDITOR AT **INSIDE SECURITY**, IT JOURNALIST,  
BUSINESS CONSULTANT, SECURITY EVANGELIST



For those of you old enough to remember the Cold War between America and the Soviet Union, these tactics seem familiar. Back then, there were constant efforts to obtain intelligence about the other side, through various spies and tradecraft now made infamous in TV and movies. But each side took the long view: when someone slipped up and revealed information, the other side took it in stride and carried on with their efforts.

That is what Internet security is these days: **a constant battle between you and everyone else**. Don't take it personally, don't give up, and don't drop your guard for even a moment. This is a war that you can win; you just have to be vigilant and prepared.

# Inbar Raz



PRINCIPAL RESEARCHER AT PERIMETERX INC.  



The Internet as we know it is not very old. The World Wide Web was invented as late as 1989, and the first browser was written the following year (source: [Wikipedia](#)). It started as a network, to connect computers around the world, but when we say “Internet Security” today it means a lot more. The term encompasses not only security issues related to the network itself (the Internet) but also security issues related to systems and infrastructures inside organizations, whether they are connected to the Internet and the outside world or not.

## How it's built

If to make a generalization, then today we are no longer looking at particular items in an organization. We look at the entire setup,



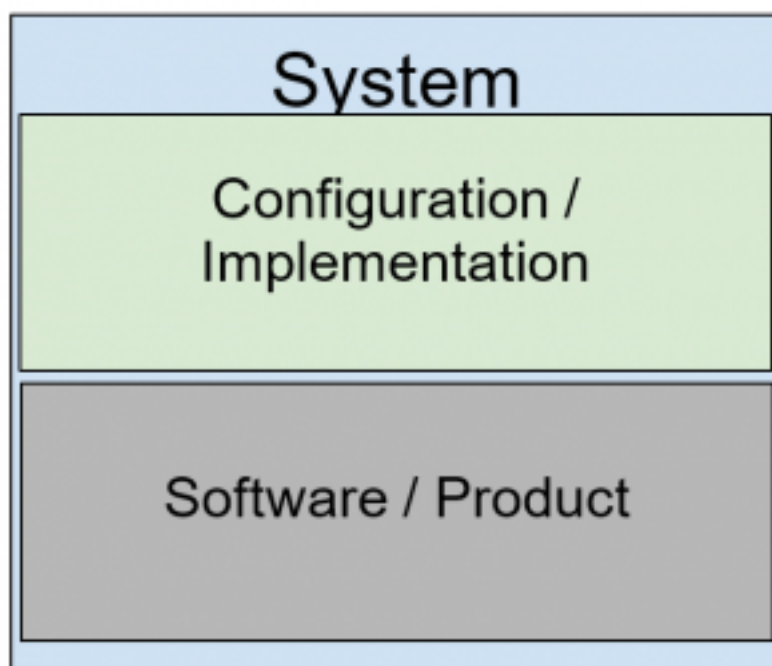
# Inbar Raz

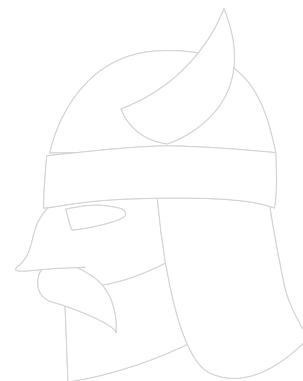
PRINCIPAL RESEARCHER AT PERIMETERX INC.  



with all its countless parts, as one big system comprised of many smaller systems.

Here's an overview of a system:





# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



A system is a compound object. At its base, it contains the Software or Product, such as a *Firewall*, a piece of *Encryption software*, or an *Anti-Virus*. Then, on top of it, lies the specific Configuration or Implementation, such as the *Firewall Policy*, the *Encryption algorithm*, and key, or the *AV Engine settings*.

The System is only as strong as the combination of the two. You can use the world's strongest symmetric stream cipher, but if your key is weak or can be broken, then the entire system collapses.

Just look at the German Enigma machine, used in World War II: Theoretically speaking, it was one of the strongest ciphers ever created and had 158,962,555,217,826,360,000 (nearly 159 quintillions) different settings



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  

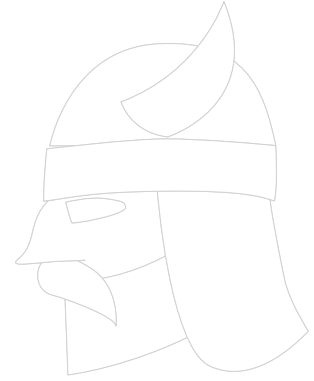


(source: [Wikipedia](#)). Even today that number is unbeatable. But it was the German procedural flaws, operator mistakes, and failure to systematically introduce changes in encryption procedures, among other reasons, that led to its demise.

Alternatively, you can have the best Firewall Policy possible for your organization, but if your Firewall is buggy or lacking features, it's just not going to do.

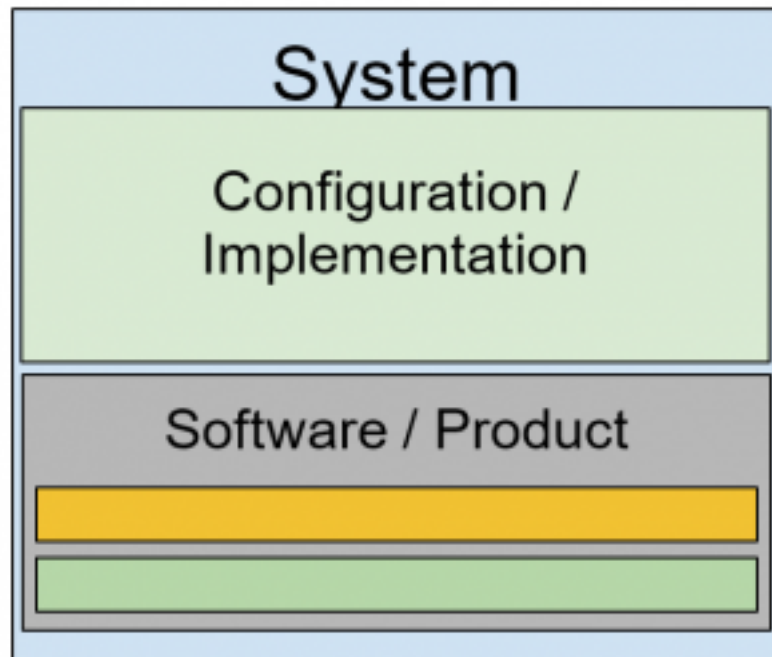
## The Problem (part 1)

The illustration used earlier was not accurate enough. The Software / Product is created by a process that I will simplify as to have two stages: The Design, and the Development.



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



Both parts of the system, the *Product* and the *Configuration*, have problems. And as mentioned earlier, either one of the parts can bring the entire system down.



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.



## CONFIGURATION / IMPLEMENTATION

There are many reasons why someone would use (or create) a bad configuration or implementation. To name just a few:

- Bad documentation;
- Good documentation that no one bothers to read (RTFM, remember?);
- Unskilled employees;
- Lazy employees (who copy & paste from Internet published examples).

## SOFTWARE / PRODUCT

Much like the System has two intertwined parts, so does the Software or the Product. If you have problems in the design, then good development won't help. If your design



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



is perfect but your developers are not, then that, too, will yield a vulnerable result. And sometimes, neither one is bad but compromises made during the process introduce vulnerabilities.

## The Solution (part 1)

Over the years, the “Internet Security” industry took upon itself to deal with all the problems caused by the various parts of the system.

In the Configuration / Implementation front, workshops and training are offered, encapsulating products were created to help you manage multiple other systems, penetration tests are performed, and more.





# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



In the Software / Product front, companies evolved to scan your products for known vulnerabilities, software upgrades are now manageable at scale, and companies even created Bug Bounty programs to help find bugs and fix them. That is, of course, in hope that hackers (or governments) haven't already found them and exploited them.

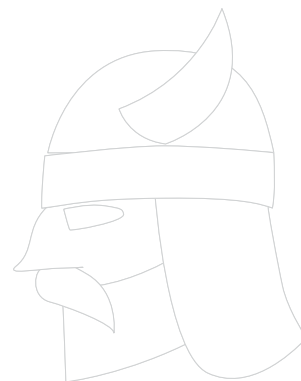
## **The Problem** (part 2)

There are many solutions. I've only named a few and there are many more which I haven't. But they all have one HUGE problem in common when it comes to the Software or Product:

**THEY DEAL WITH PROBLEMS THAT ARE ALREADY THERE. THEY DON'T PREVENT**

# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  

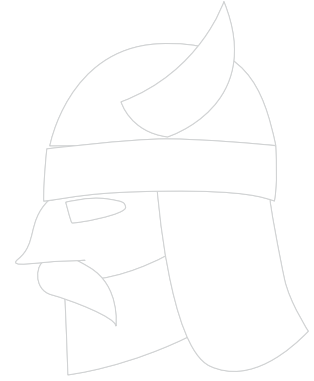


## NEW PROBLEMS FROM EMERGING.

There is a HUGE quality problem here. Companies and vendors keep producing vulnerable products, and the security industry keeps chasing its own tail, as well as that of the vendors, trying to plug all the holes in the dam.

### **The Solution** (part 2)

Companies and Vendors know all that, and they are not sitting on their hands. Secure Development Lifecycle methodologies were created, and in some cases (though not nearly enough) there is actually someone in charge of Security in the Design stage. More and more companies are even embracing the Bug Bounty programs, or even just Coor-



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



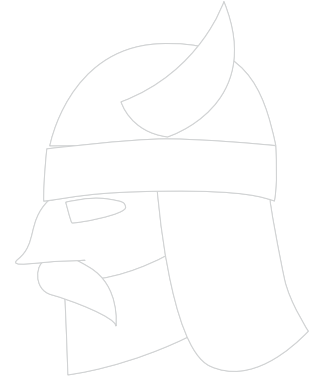
minated or Responsible Disclosure policies. But that is not nearly enough. And here's why.

## **The Problem** (part 3)

There are not enough incentives for making a better, more secure product, and at the same time, there is little to no liability for vendors whose vulnerable products were exploited.

**AND HERE LIES THE REAL PROBLEM.**

Think about it: The vast majority of PCs and Servers are running Microsoft Windows. Almost all versions ever were found to be vulnerable, and I don't have exact data but I'm willing to bet that every single version



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  

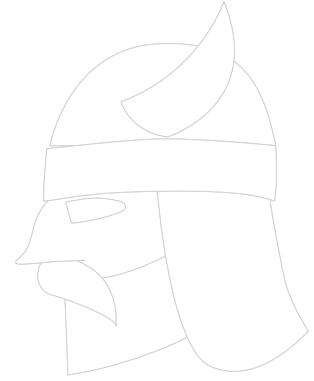


was used in a hack.

*How many infected emails include a malicious Acrobat PDF file? Or a Macro-enabled / Exploit-infused Microsoft Office file? How many Java applications have been found to be vulnerable and exploited? How much money was lost in all of those attacks?*

But no one is holding Microsoft, Adobe or Oracle accountable. In comparison, when a car manufacturer produces a faulty car and accidents happen (sometimes killing people), the vendor is subject to criminal investigation and prosecution, not to mention civil suit. But no one ever comes after the software vendors. *Why?*

In the eternal race to the customer's choice,



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



companies prefer to release an early, immature product, counting on the fact that if vulnerabilities are found, they will simply issue a fix. The customer won't switch products.

So Time-to-Market is more important than Security. And this is why buggy and vulnerable software keeps shipping out, creating a world of problems that everyone else is trying to deal with.

## **The Solution** (part 3)

And here comes the hard part, also known as "Easier said than done".

COMPANIES AND VENDORS NEED TO BE HELD ACCOUNTABLE FOR THEIR PROD-



# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



UCTS.

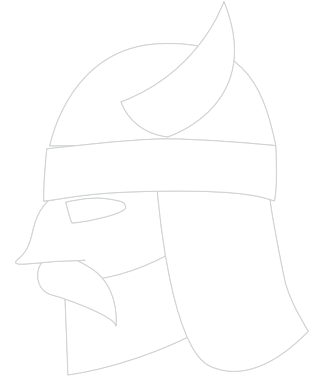
If your software was vulnerable and was used to hack into my system and steal my money or data, you are responsible for it. You need to be liable both criminally and in civil court since it was you who facilitated the hack. If you can prove that you went the extra mile to try to prevent bugs, then that's one thing. But if you didn't, will, cough up the money.

## Conclusion

*So, is Internet Security a Losing Battle?*

Yes, it is.

As long as we are not addressing the prob-



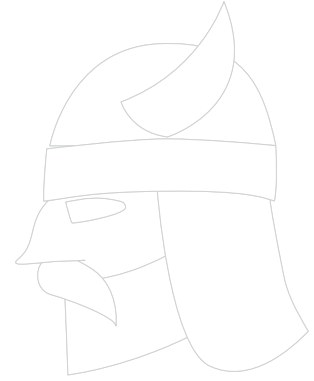
# Inbar Raz

PRINCIPAL RESEARCHER AT PERIMETERX INC.  



lem of bad Software and Product development, more vulnerable software will come out, and we will all keep chasing the problems. And yes, Internet Security will keep being a losing battle.

The moment that we shift the responsibility to the vendors, and give them a good incentive to create better products (fear is also a good incentive), then we stand a chance. And if we ever get to that point, ask me this question again.



# Jeff M. Spivey

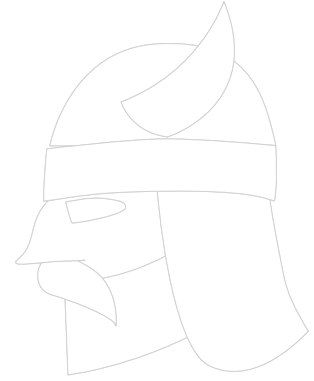
CRISC, CPP, BOARD DIRECTOR OF ISACA AND  
FOUNDER AND CEO OF SECURITY RISK MANAGEMENT, INC.



**Internet security is not a “losing battle”** but I suggest it is a longer-term war requiring organizations to be very curious and aware of all internet security-related risk to their organization. The success of this “war” will be measured by the maturity of the security risk management framework employed by the organization, including its agile and dynamic understanding of threats, vulnerabilities and risk management principles employed.

The threatscape is so dynamic that one-off solutions relating only to technology are ineffective and will only bring temporary and limited success. Establishing a framework is the key to the long-term internet/digital/cyber security risk management survival of the organization.





# Jeff M. Spivey

CRISC, CPP, BOARD DIRECTOR OF ISACA AND  
FOUNDER AND CEO OF SECURITY RISK MANAGEMENT, INC.



Three major strategies will help reduce the impact and likelihood of security risks to our organizations:

1. **Understand the major frameworks for security risk management models, including COBIT and NIST.** Using these as a foundation, design and implement the specific model that fits with your organization's culture, the maturity of business processes and existing enterprise risk management program.
2. **Technology consumers must demand sound security be built into all new technologies before being allowed to sell the technology.** Everyone and every organization should require proof of security capabilities before purchasing new technology. The

# Jeff M. Spivey

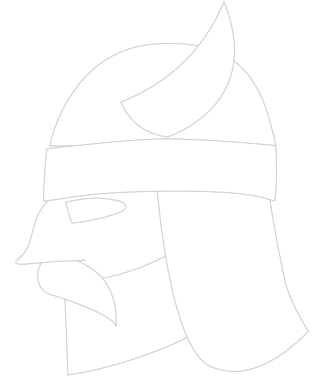
CRISC, CPP, BOARD DIRECTOR OF ISACA AND  
FOUNDER AND CEO OF SECURITY RISK MANAGEMENT, INC.



manufacturers will then make secure devices from the beginning and strengthen our technology ecosystem.

3. **Prior to being sold, all new technologies (Internet of Things, Chips, FinTech, etc.) should have a mandatory review to assure adherence to a set of security standards affecting increased risk to organizations.**

**Internet Security is like world peace – you will conquer some of what you focus on, but the world’s security risk still varies from battle to battle.** To secure your part of the world, you must have a security risk management framework adapted to your organization, dynamically discovering and managing security risk both inside and outside the firewall.



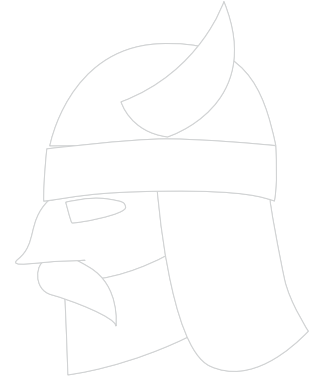
# Joaquín Pérez Ruiz

IT CONTROL & RISK MANAGER



Nowadays, it is fairly common to hear about a company that has been hacked, personal information disclosed, financial scams, or even, about money being stolen from banks. This has become so commonplace that is not surprising anymore.

We could think that cyber security is something applicable only to businesses, as they are targeted most visibly by cyber criminals, but this is no longer true as we live in an interconnected world and everyone has become a target for cyber criminals. In fact, they can use wide range scans of the internet to look for vulnerable systems. As soon as they find one (that could be your phone, smart TV, home router or even your fancy new refrigerator connected to the internet), they can break in and take control of the



# Joaquín Pérez Ruiz

IT CONTROL & RISK MANAGER



system.

In order to be protected and increase the safety of the internet as a whole, it is very important to **focus on the security culture**, because we cannot predict the potential impact of such attacks on us as single users and each of us is targeted by cyber criminals. We have all heard about cyber scams, cyber extortion, identity theft and many other tactics cybercriminals use to profit from their actions.

The security culture should be promoted at several levels in order to reach the widest audience and be effective as the first line of defense:

**Personal cyber security awareness:**



# Joaquín Pérez Ruiz

IT CONTROL & RISK MANAGER



- Know how many devices you own that are connected to the internet.
- Apply the best practices of password security (use strong password, change passwords set by default in devices, avoid reusing passwords and so on)
- Take care of your devices and ensure that the latest firmware updates and patches are applied.

## **Companies' cyber security awareness program:**

Companies need to reinforce the cyber security messages to their employees, not just to protect themselves, but to make the internet a safer place as a part of their corporate



# Joaquín Pérez Ruiz

IT CONTROL & RISK MANAGER



social responsibility programs.

## **Manufacturer's responsibility:**

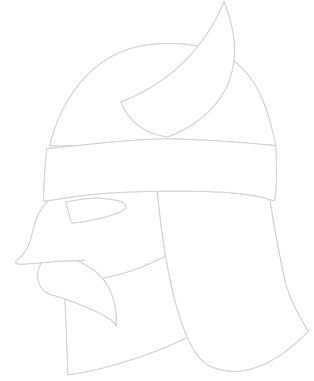
Manufacturers need to take responsibility for their devices and ensure that they are producing secure devices that comply with the minimum security requirements in order to avoid cyber criminals taking advantage of security flaws included on devices.

## **Governments' awareness plans:**

Nowadays cyber security is a global problem that needs to be managed as a global risk, so, governments need to be involved in developing the cyber security culture in order to minimize the impact of cyber-crime by creating the appropriate laws, investing in

# Joaquín Pérez Ruiz

IT CONTROL & RISK MANAGER



cyber security and even developing a cyber security awareness program.

**Cyber security is not just a technical problem, it is the responsibility of every connected person, and so, everyone needs to do their part if we want to be safe in an interconnected world and win the battle against cyber criminals.**



# Kevin Townsend

FREELANCE JOURNALIST AND WRITER WITH MORE THAN  
10 YEARS' EXPERIENCE IN WRITING ABOUT SECURITY ISSUES

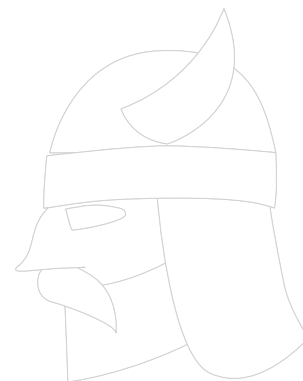


## Is internet security a losing battle? – A consumer's perspective

**Internet security is not a losing battle; it is a continuing battle.** We have not eradicated burglary in the physical world despite the size and resources of our police forces – but most of us, especially those who take sufficient care – have never been burgled. The internet is similar – **we will never eradicate cyber crime, but we can take steps to reduce the likelihood of it happening to us.** We cannot win, but that doesn't mean we have to lose.

In the physical world, there is a police concept called CPTED: Crime Prevention Through Environmental Design. The idea is simple: we can build or develop a structure





# Kevin Townsend

FREELANCE JOURNALIST AND WRITER WITH MORE THAN  
10 YEARS' EXPERIENCE IN WRITING ABOUT SECURITY ISSUES



that becomes sufficiently difficult to burgle that the burglar moves on to a different and easier target. It doesn't eliminate burglary, but it makes it less likely for those who take care to be burgled. By adopting a similar approach to our own internet experience we can make it too difficult for all but the most determined cyber attacker.

**On the internet, there are three types of attacker that we must at least be aware of:**

- the simple criminal who steals our data for profit;
- the software vendor who openly or covertly takes our data for profit;
- and the governments who take our data for control purposes.

# Kevin Townsend

FREELANCE JOURNALIST AND WRITER WITH MORE THAN  
10 YEARS' EXPERIENCE IN WRITING ABOUT SECURITY ISSUES



All three require a different response:

- **criminal:** up to date anti-virus; install all patches as they become available; don't click on links in unexpected emails, nor open unexpected attachments; avoid visiting dubious sites; use a password manager to generate unique strong passwords for different accounts (and use multi-factor authentication wherever possible); have a separate account with minimal funds for online shopping and check for the padlock icon; choose cloud storage with care, using encryption wherever possible; and don't be over garrulous on social media.
- **software vendor:** there's not much we can do here, but use reliable app stores, read the end-user license, and lock down all op-



# Kevin Townsend

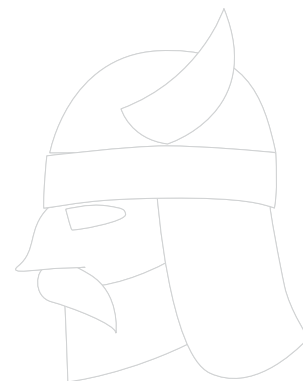
FREELANCE JOURNALIST AND WRITER WITH MORE THAN  
10 YEARS' EXPERIENCE IN WRITING ABOUT SECURITY ISSUES



tions available. If we think the software seeks to take more information than is necessary, we can reject it and go elsewhere.

- **government:** and there's even less we can do here, assuming we actually want to. Don't just accept encrypted services – specifically look for 'end-to-end encryption' for our communications. If we worry about our ISP monitoring our internet viewing practices (either to pass to government or to sell to marketing companies) we can use a VPN.

None of this will guarantee our safety on the internet – but in combination, they will keep most of us safe enough most of the time.



# Lawrence Abrams

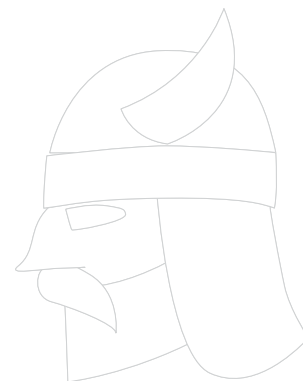
OWNER AT BLEEPING COMPUTER



**Security is only a losing battle if someone allows it.** I think anyone can keep their computers and networks protected if they follow good security and computing practices. If not, then they open themselves up to risk for a myriad of attacks including malware, identity theft, and credential stealing.

*So what should an individual do to protect themselves?*

1. If you use Windows, you should do is **enable the viewing of file extensions** (<https://www.bleepingcomputer.com/tutorials/how-to-show-file-extensions-in-windows/>). For some silly reason, Microsoft decided to make it so users do not see file extensions by default. This allows malware executables to disguise themselves as normal



# Lawrence Abrams

OWNER AT BLEEPING COMPUTER



data documents such as office documents and PDF files, which people open without realizing they are actually opening and executing a malware file.

2. **Use a unique password at every site you visit.** We hear almost every day about large data breaches where people's usernames and passwords are leaked. If you use this same username and password at other sites, hackers can use them to try and access bank, email, and other personal accounts. I strongly suggest that everyone use a password manager to keep track of the unique passwords that are used at each site.
3. **Do not open attachments you receive via email without confirming with the sender that they actually sent you one.**



# Lawrence Abrams

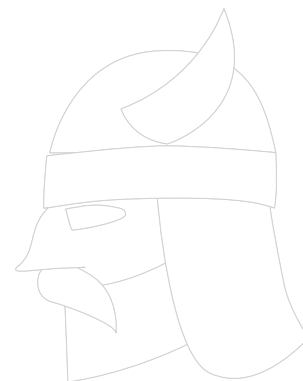
OWNER AT BLEEPING COMPUTER



Ransomware and other malware are commonly sent as attachments that pretend to be invoices, complaints, shipping confirmation, voice mails, and even faxes. If you are unsure if someone sent you an attachment, you should download it and scan it with a service like VirusTotal before you open it.

4. **Do not use weak passwords.** I know it's easier to use 123456 as your password, but that also makes it easy for criminals to guess it too. Use a password manager as suggested in step 2 and you will never need to worry about remembering hard passwords again.

5. **Use 2 Factor authentication to secure your online accounts.** 2 Factor authentication is when you not only need to



# Lawrence Abrams

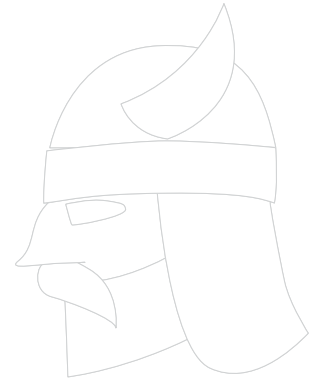
OWNER AT BLEEPING COMPUTER



know your password, but also need a device such as a mobile phone to help authenticate you into an online account. As only you will have possession of your phone, even if hackers guess your password they still would not be able to log in.

6. Last, but not least, **be careful what you download from the Internet**. Many free programs are bundled with adware, PUPs, or even Trojans that can cause severe issues on a computer. Therefore, when downloading a free program from the Internet pay close attention to license agreements and default programs that are being installed to make sure they are not installing something unwanted as well.

If you follow these steps, your computer and



# Lawrence Abrams

OWNER AT BLEEPING COMPUTER

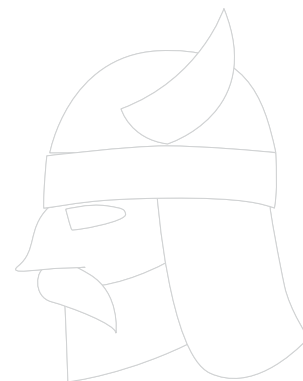


network will be safe, and you will actually win the battle in security.



# Liviu Arsene

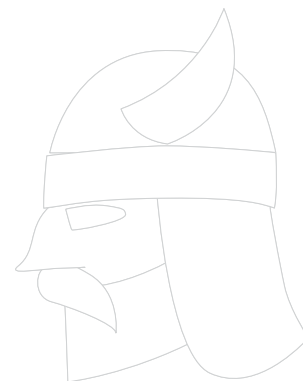
SENIOR E-THREAT ANALYST AT BITDEFENDER



**Securing the internet is not a losing battle as long as we want to enjoy the same freedom of sharing and accessing information.** While security plays a vital role in ensuring that freedom, the challenges brought forward by securing freedom are well worth it.

Granted, the rapid pace at which we adopt new technologies and connect devices to the internet's infrastructure are placing a constant strain on the backbone of what we call "the internet", but giving up is not necessarily an option.

For instance, new technologies can be developed to secure the ever-growing number of IoT devices. New protocols and new hardware can be developed to support the high-volume throughput generated by the



# Liviu Arsene

SENIOR E-THREAT ANALYST AT BITDEFENDER



billions of internet-connected devices.

Simply giving up and saying that securing this expanding interconnected infrastructure, with its services, technologies, and hardware, is not an option. Not because we can't live without them, but because solving these challenges will help us constantly innovate and advance the way we interact with each other.

The internet is vital and the more it expands, the more we need to make sure that data, security, availability, and accessibility are not hindered or impaired. If we've learned anything since the internet began is that **new technologies and figuring out how to properly use them requires time, commitment and collective effort.**



# Mădălin Dogaru

CEO & FOUNDER AT SENTIENTCHIP 



This is a very difficult question as there is no easy answer. To be able to answer it, we first need to understand how the battle began.

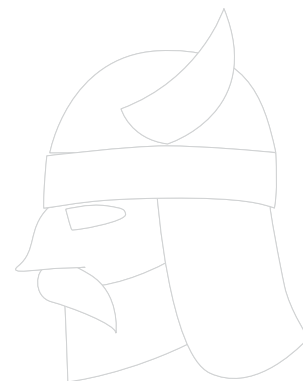
## Birth of the Internet

The first form of a primitive Internet appeared in 1969 and it was named ARPANET (initially a US military project). It interconnected multiple computer networks together into a bigger network and allowed communication between them.

Later in 1982, the TCP/IP Internet protocol suite became the standard networking protocol in ARPANET. The first ISP's appeared around 1989, just before ARPANET was decommissioned in 1990.

# Mădălin Dogaru

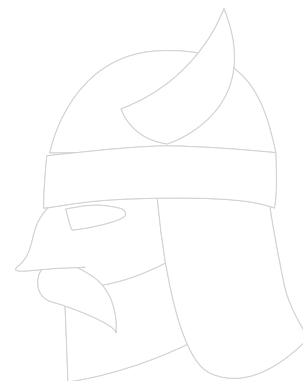
CEO & FOUNDER AT SENTIENTCHIP



In the same time, in 1990, Tim Berners-Lee presents the World Wide Web (www) information space and in 1993 the first browser is born under the name “Mosaic”. Later in 1995 the Internet explodes and begins influencing the whole world through VoIP, instant messaging, electronic mail or video calls.

## Computer/Network Hacking in this period

Hacking in this period was seen as positive thing because it was (and still is) about curiosity and learning how a system works (although it annoyed companies). But from this branch emerged the “Cracker” who is malicious and destroys systems and software. Later people associated Cracker with Hacker and thus the current bad reputation.



# Mădălin Dogaru

CEO & FOUNDER AT SENTIENTCHIP

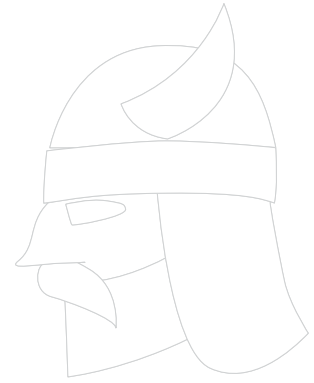


In 1965 William Mathews D. from the Massachusetts Institute of Technology discovered a vulnerability on the IBM 7094 model. The default text editor on the system was written in such way that it could be used by one user at a time and in a single directory. By using the application in the same time by two users, the temporary files for “Message of the Day” and the password file became swapped. As a result, the password was displayed on the screen for everyone using that system.

1981 sees the birth of a few hacking groups (The Warlords in the US, Chaos Computer Club in Germany). Later that year Ian Murphy (Captain Zap) becomes the first cracker to become convicted after breaking in AT&T and modified the internal clocks that me-

# Mădălin Dogaru

CEO & FOUNDER AT SENTIENTCHIP

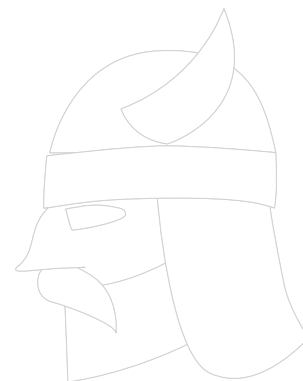


tered the phone calls billing rates. As a result, people that waited until midnight to make phone calls (at midnight usually was cheaper) got hit by heavy bills.

From 1983 to 1986 the increase of attacks on networks rose significantly (with companies losing money this time), causing the US government to pass the Computer Fraud and Abused Act (in 1986) which made it a crime to break into a computer system.

From 1986 to 1990 arrests increased, crackers caused mass disruption of systems, first computer worms appeared (e.g. Morris Worm) and CERT was created (1988) by DARPA.

## Past, Present and Future



# Mădălin Dogaru

CEO & FOUNDER AT SENTIENTCHIP

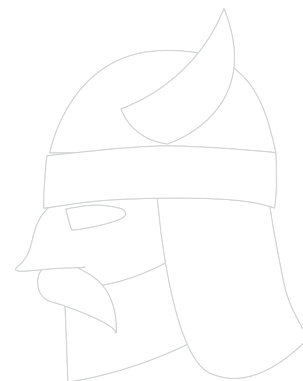


The reason I gave a few details about what happened until 1990 was to show that Hacking was and still is a culture focused solving problems and improving things. Yes, from time to time Hackers annoyed companies and governments with their break-ins and pranks but it was not so serious. Mostly because the intent was not malicious, they just wanted to see if they can do it.

Starting with 1990 things changed completely. Strong cracking groups begin attacking specifically for money gains, malware is released with destruction in mind or as backdoors for future attacks, first bank attacks appear (e.g. Russian groups steal \$10 million from Citibank), DOS is born, government networks are breached and companies lose huge amounts of money.

# Mădălin Dogaru

CEO & FOUNDER AT SENTIENTCHIP

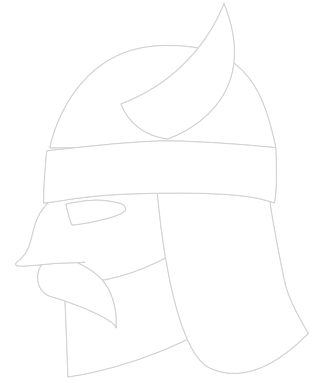


The rate of attacks increased until the present at an incredible rate, mostly due to the involvement of the mafia which use individuals with good computer skills to help them steal credit cards information, develop ransomware business models (yes it is a business model, and a good one) or plant Trojans in banks to suck money at a small and steady pace.

Now returning to the question “Is Internet security a losing battle?”, I must admit that things don’t look so good because:

- most security companies milk their security solutions as much as possible while attacks evolve at an incredible rate.
- a lot of big companies and banks still





# Mădălin Dogaru

CEO & FOUNDER AT SENTIENTCHIP

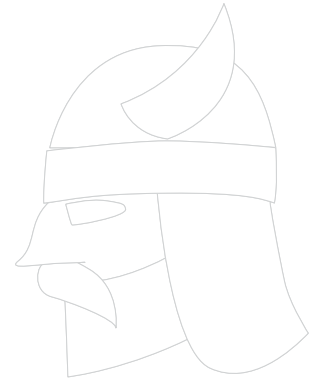


work based on the “we spend more on enforcing security than what we lose in case of a breach” principle and they apply minimum security measures.

- security awareness is mostly based on presentations of attacks “don’t open emails from people you don’t know”, which is useless as the whole point of a spoofing attack is to mimic a friend or colleague. Security awareness is made by involving the employee in hands-on example attacks (showing them how the attack is performed) and hands on defense (showing them how to defend).
- penetration tests are made based on tons of rules (you can’t social engineer that person, you can’t attack during the night

# Mădălin Dogaru

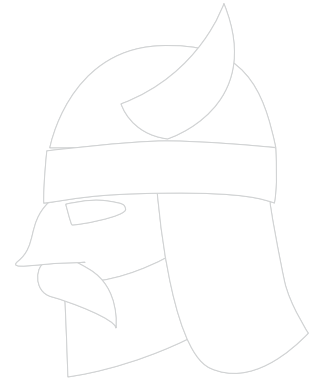
CEO & FOUNDER AT SENTIENTCHIP



etc). This reduces its effectiveness greatly.  
*Do you think crackers play by the rules?*

- the WWW was by default not made to be safe, it was built to exchange information. We need WWW 2.0 if we want a big boost in security (nothing will ever be 100% safe) but until then, the shift must be made faster towards SDN (Software defined networks).
- big companies need to improve their structures because they react very slowly to technology changes, thus by the time they update their systems, new attacks already appeared.

It's a big subject on which we can talk for days and the answer is that **the battle is not lost but we are indeed losing**. That being



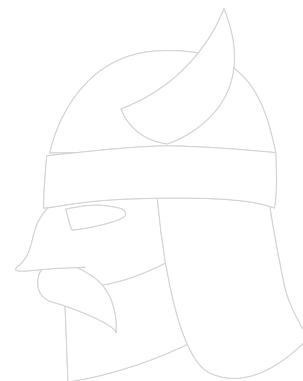
# Mădălin Dogaru

CEO & FOUNDER AT SENTIENTCHIP



said the “good guys” are lagging behind because they have to obey some hindering rules, business is still put before security, true security awareness is still a small percentage of the pie and security providers are copying each other (e.g. basic antivirus solutions are still emerging) instead of innovating.

Right now, basic forms of A.I. are being developed and in the near future the war will probably be a duo of attacker + specialized A.I. versus a defender and his A.I. But we will have to wait and see.



# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION

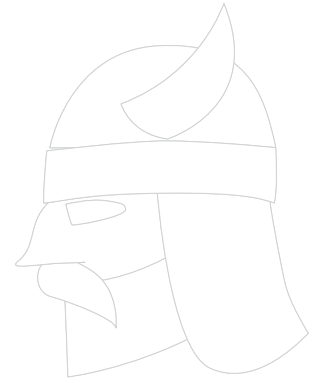


## 3 Reasons Why is Cybersecurity Losing

Cyber threats are currently outpacing the defenders but it does not need to be the case. Attacks are increasing in number and type, with the overall impacts are becoming greater. Cyber security is struggling to keep our digital lives and assets protected from the onslaught of attacks but facing great challenges. By understanding the root causes, we can adapt and change the equation for everyone's benefit.

**There are three aspects which are contributing to security currently losing the battle against cyber threats:**

1. Rapid growth and importance of the



# Matthew Rosenquist

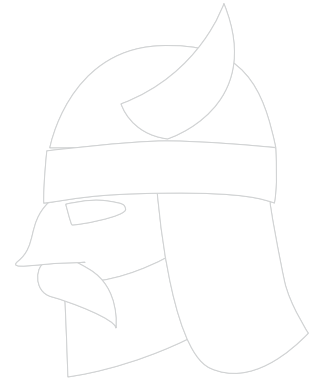
CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



technology landscape in people's lives

2. Rising complexity, costs, and organizational challenges for defenders
3. The improvement of attacker's tools, capabilities, and collaboration.

Combined, this situation creates an environment like a perfect storm, enabling the threats to outpace and outmaneuver current defenses. This is driving changes to expectations and market forces, which will fuel more security innovation and acceptance into play. Out of the chaos, we will ultimately see a new equilibrium established where the risks, costs, and usability of technology are at an acceptable level for our security, safety, and privacy. It is up to the security



# Matthew Rosenquist

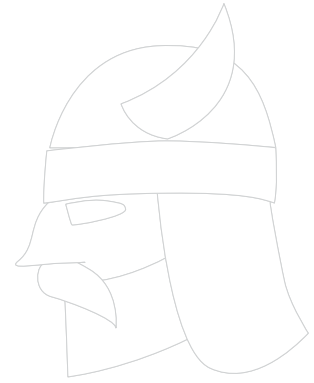
CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



industry and public to decide how fast we get there and what that optimal balance will look like.

## RAPID GROWTH AND IMPORTANCE OF THE TECHNOLOGY LANDSCAPE

The Internet is getting crowded with the proliferation of new users, devices, and usages. Over a billion more people and tens of billions of devices will get connected online in the next few years. New users are typically not very security savvy, making them easy prey for spam, phishing scams, and even the most basic malware. More websites and online services will sprout up to meet the demands and take advantage of these new markets. **In the rush to connect, security tends to fall to the wayside**, as busi-



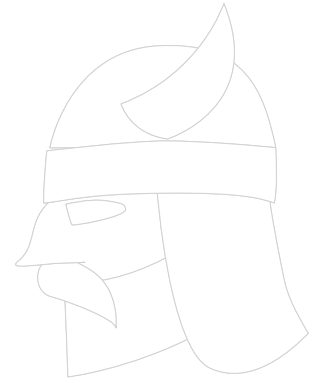
# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



nesses prioritize market position and visibility over protective controls.

The Internet-of-Things (IoT) will comprise the vast majority of new devices, with some estimates exceeding 20 billion by 2020. These are not fully fledged computers like the PC's, laptops, tablets, and phones which are designed to run lots of different software and support advanced security capabilities. Instead, these IoT devices are more specialized to specific functions. Televisions, cameras, DVR's, automobiles, kitchen appliances, medical devices, industrial sensors, and even clothing will all be connected to the Internet. They will gather data and process commands, but in a limited way. Every imaginable type of normal machines we use today will be enabled to communicate and in



# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



many cases be controlled remotely.

This opens up tremendous new usages and experiences for the benefit of users. Imagine wearable or implantable medical sensors which monitor health and intervene when needed to save lives. Autonomous vehicles will transport passengers wherever they desire, while they focus on other activities. Fully automated homes will configure and stock themselves for the customized needs of its occupants. It is an exciting time where technology will connect and enrich the lives of people all over the globe, but there are risks.

**For every new usage, connection, or technology tool, there is a risk it may be used against us by cyber threats. Those same**





# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT [INTEL CORPORATION](#)



connected devices can be controlled by hackers for a variety of nefarious purposes, none of which are for our benefit. As we relinquish control of certain aspects that could pose life-safety risks, such as transportation, healthcare, and industrial functions, we inadvertently trust our safety to devices which may be maliciously manipulated by others. Autonomous transportation is a wonderful advancement, as long as it is not hacked, resulting in crashes and fatalities. Medical devices and data could be altered, resulting in catastrophic outcomes.

Even simple home devices are at risk. We have seen a flood of recent attacks against IoT devices where cyber criminals are taking them over to be used as part of a botnet. These botnets can cause parts of the Inter-



# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION

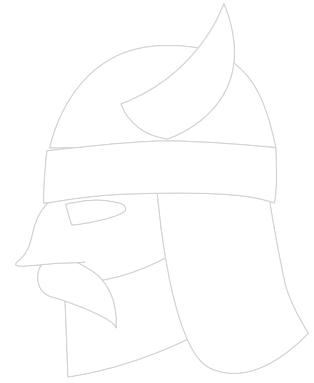


net to crash, take down specific websites, support illicit markets, create fraudulent social media accounts, and harvest personal data of their owners.

This is just the beginning. As our technology ecosystem continues to grow at breakneck speed, with more devices, users, and usages, we create an environment rich with easy targets and capabilities crucial to our security, safety, and privacy.

## **RISING COMPLEXITY, COSTS, AND ORGANIZATIONAL CHALLENGES FOR DEFENDERS**

Businesses, governments, organizations and individuals struggle with the complexity, costs, and knowledge necessary to improve security, safety, and privacy. Cyber security



# Matthew Rosenquist

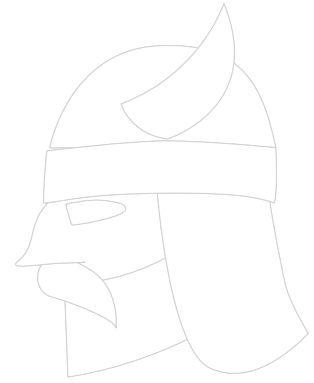
CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



is not easy to understand. It must comprehend the technology, threats, and varying demands of users. It is a complex challenge within a constantly changing chaotic environment.

**Security must protect the breadth and depth of the technology landscape at every place data exists, is being transported, or is in use.** Any weakness will be exploited. Like a fence, it must protect against all the locations of attack and be high and strong enough to repel the craftiness and persistence of outsiders trying to get in.

Cyber threats are intelligent adversaries who are driven by motivations to achieve their objectives and are both creative and relentless. This challenge creates a desire by de-



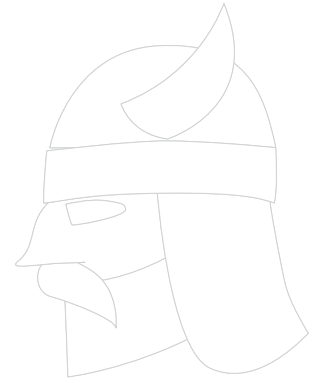
# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



fenders to institute massive and formidable controls, but that would greatly impede the end user's desired functionality and performance of these systems. **Every good security program must align with the ever-changing expectations of users, within the limits of what is possible and at a reasonable cost.**

Security is only desirable when there is a perception or reality of negative impacts. Risks are the expected impacts over time. As no system is perfect, there will always be some losses, therefore some risk. **The key is to reach an optimal level where the costs of security achieve an acceptable level of risk and usability.** Cyber security must strive to identify where this point is, but is stymied as future losses are near impossible to estimate. Much of the industry is based upon



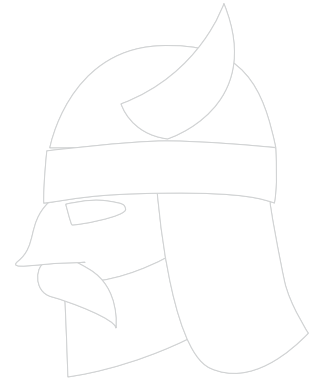
# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT [INTEL CORPORATION](#)



fear, even if it is supported by numerous incidents, examples, and a tremendous amount of data. The perception of risk is a very personal matter. It makes the job of protecting computing systems, that service many people, very challenging.

Other requirements are clearer, such as regulations which govern specific industries, technology, and services. There are two main problems in being compliant with such laws. First, there is a multitude of different regulations from across the globe. With little consistency, it is a costly challenge to remain aware of changes and to comply with them all. Then there is the second, more important aspect, as compliance does not equate to being secure. One of the biggest misconceptions is that adherence to



# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



regulations will ensure security. This is simply not true. In fact, most major breaches are with companies which have to meet required standards. Regulations are simply the lowest acceptable level of basic controls. They should be considered the starting point, not the end state of a good security program.

**The last major challenge is understanding what should be done.** This requires talented individuals to understand the risks, the technical environment to be protected, and the user's expectations which must be satisfied. They must determine the best technical solutions, behavioral policies, and process controls. It is no easy task.

Security professionals are in great demand



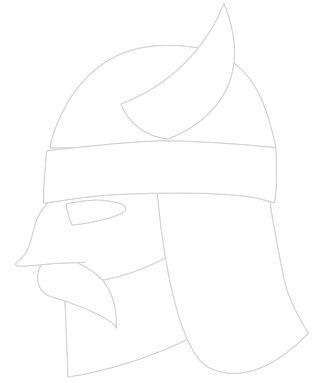
# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



as the technology landscape continues to rapidly grow. This has created a tremendous market with very few capable people to fill all the roles. Cybersecurity is a relatively new field. Only in the past few years have higher education institutions recognized the need. Academia is rushing to establish programs to train the next generation of cybersecurity professionals. In the meantime, there are an estimated 1 to 2 million unfilled positions. This gap will likely grow before supply begins to reduce the number of vacancies.

The result is most organizations do not have the necessary talent to secure their products, services, infrastructure, or assets. The costs, complexity, and lack of talent make cyber security a tremendous challenge to



# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



tackle. Although many organizations have chosen to ignore the risks in the past, the new devices, usages, and expectations are forcing recognition, accountability, and a real commitment to security, safety, and privacy.

## THE IMPROVEMENT OF ATTACKER'S TOOLS, CAPABILITIES, AND COLLABORATION

Cyber threats consist of a broad community of different Threat Agents (TA). Archetypes range from thieves, hackers, organized criminals, hacktivists, and even nation-states. Some act alone with little skill, while others have vast resources at their disposal. The most advanced threats possess expertise in both technical and behavioral disciplines.





# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



**Most threats, however, are simply reusing or customizing tools and methods developed by others.** Overall, it is a diverse community, vast and global in nature, which has the tremendous collective power to disrupt, steal, undermine, and take control of computing assets anywhere in the world. These intelligent adversaries are what makes cybersecurity truly challenging, and they are getting better every day.

**The key to threats agents is their motivations.** Every potential attacker is driven by an internal drive which dictates the objectives they will pursue. Activists want to change in the world, criminals want financial gain, disgruntled employees want revenge, nation-states want to influence political and military outcomes, and so on. These people



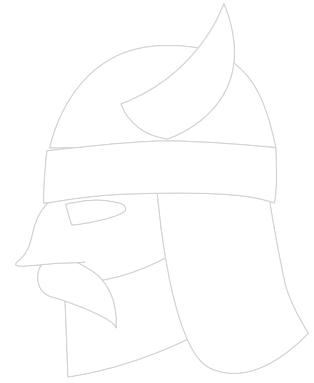
# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



and groups have always been part of society, but with the rise of technology they see hacking as a set of new opportunities. So they leverage weaknesses in the electronic ecosystem to achieve objectives that satiate their motivations. The apparent ease and bountiful rewards fuel these acts, reinforcing the behaviors, and forging continued persistence. These threats are at the heart of every cyber-attack.

**Every piece of technology is simply a tool, which can be used for good or for malice, and cyber threats are masters at using tools.** This is a huge advantage attackers have over defenders. The more complex and capable a device or service, the more opportunities for hackers to find a way to undermine, compromise, or misuse it. So the rise



# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



in our technology landscape simply opens tremendous doors for those looking to conduct attacks.

**Successful attacks reinforce the behaviors with rewards and supply more resources for the threats to use in follow-on activities.**

Hacking a network exposes systems behind it. Successful ransomware campaigns return financial assets which can be reinvested. Stealing user credentials then allows access to those resources and the ability to impersonate others.

Rewards can be significant. A recent analysis of the ransomware campaign Cryptowall v3 showed how one cybercriminal crew was able to successfully extort over \$300 million from victims in a short period of time. The



# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



greed of thieves is insatiable, which prompted a version 4 to be released shortly thereafter. With such successes, there is no end in sight to ransomware activities.

**One major difference between the attacker and security communities is the willingness to share information.** The hacking community has a long history of sharing code, best practices, victim data, and assisting each other in overcoming barriers. They actively help each other with problems and openly give advice. There is very little perceived competition which opens the floodgates for a community to actively collaborate. Security companies, businesses, and even governments, on the other hand, have shown little desire to share information or work together in practical ways. Only recently has some of



# Matthew Rosenquist

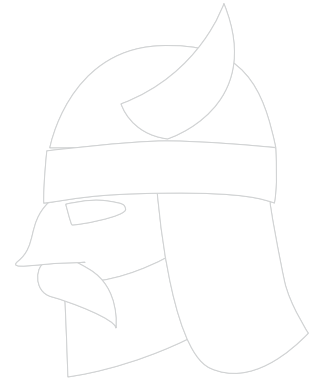
CYBERSECURITY STRATEGIST AND EVANGELIST AT [INTEL CORPORATION](#)



the isolation been removed and security groups are slowly beginning to share threat and attack data. Still seen as competitive or potentially impactful to customer confidence, most companies remain pensive. The result is a major barrier to innovation, intelligence, and collaboration for security. This disparity between how these two communities act provides a huge advantage to the attackers. They work together to share knowledge and resources. Until the good guys can set aside apprehensions, it is unlikely they will ever be able to keep pace with an ever-growing and powerful hacking community.

## TURNING THE TIDE

The challenges are now daunting and



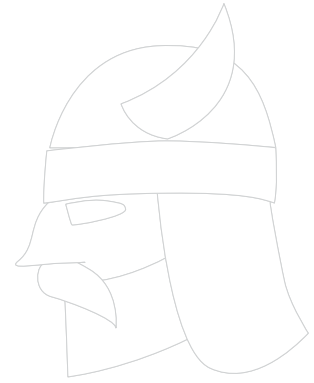
# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



changes must be made to slow the attackers' pace while accelerating protection capabilities. Recent reports estimate the overall damages of cybercrime will reach \$6 trillion by 2021. Malware is currently being created at a mind-boggling rate of 400 thousand new samples each day. **2016 will likely be the worst year for data breaches and we have only begun to feel the pain of IoT attacks.**

**Consumers, businesses, and governments all play a role in making security better.** Consumers must take the security of their devices and assets more seriously. This includes proper digital hygiene of good password management, using quality security solutions, only installing trusted software, and keeping systems updated with latest patch-



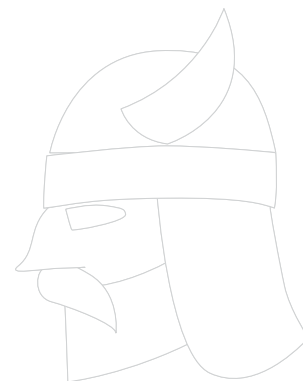
# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



es. They must be critical before opening potentially harmful messages, attachments, texts, and web links. Most importantly, consumers should make security and trust a factor in their purchasing criteria for new products. Voting with their wallets, to reward those companies that invest in good security practices, is a powerful force to drive more secure products.

Businesses must raise cyber security to an executive level necessary for responsibility and accountability. They must invest not only in protecting the business infrastructure but also their products and services. Having a well-trained and resourced team is required to build and sustain a security program.



# Matthew Rosenquist

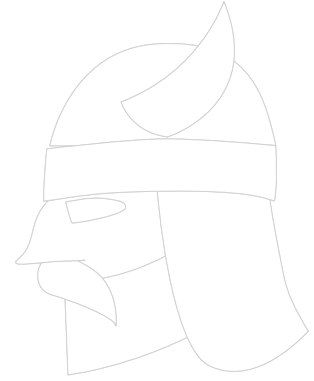
CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



Institutions and industry sectors must share more information on threats, attacks, and best-known practices. Security is a collaborative effort. It is the good guys against the threat agents. Without teamwork, we don't stand a chance against the attackers.

Governments must unify and make regulations easier to understand. They are a part of the picture but do not satisfy the entire need. Organizations must be compliant as a start but continue to pursue more advanced controls as they seek an optimal balance of security. Improvements in law enforcement's ability to investigate attacks and prosecute offenders are also needed within and across jurisdictions. **Cybercrime is a global epidemic, not bound by traditional borders.**



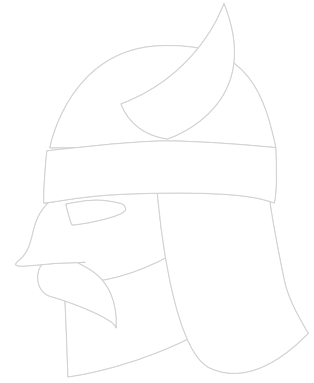


# Matthew Rosenquist

CYBERSECURITY STRATEGIST AND EVANGELIST AT INTEL CORPORATION



Overall, we must all work to protect the safety, security, and privacy of our data and community. We must maneuver with forethought as this problem will not go away on its own. We are all participants and custodians of the internet connected world. **It is time we step up and collectively fulfill our roles as members of the digital society and work together to make it a more secure place.**



# Morten Kjaersgaard

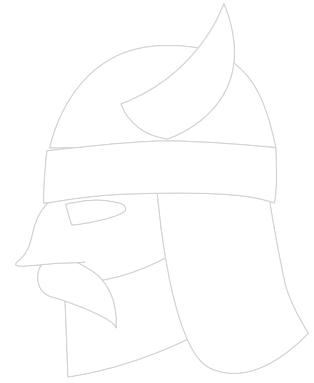
CEO AT HEIMDAL SECURITY



Whether internet security is a losing battle or not is very hard to answer. I see many things comparable to that of other industries, where things evolve quicker than humans can adapt.

The invention of the automobile being a very simple example. Nobody got killed by the speed of the first cars, but if you look at the market today the top speed of the car evolved much faster over the '70s, '80s, '90s, 00's than the security of cars could keep up. The same has happened on the internet.

The car industry was in many ways legally forced to adapt, at least in Europe with the NCAP scoring being introduced as well as a number of minimum requirements for security. The same has also applied in the US in



# Morten Kjaersgaard

CEO AT HEIMDAL SECURITY 

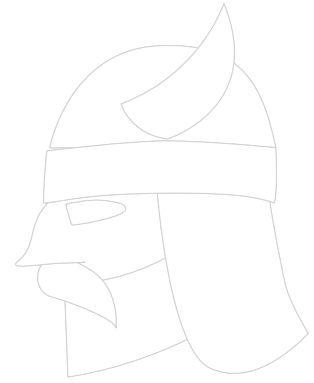


different ways.

I foresee the same will happen with the Internet and the security space surrounding it. The EU GDPR (General Data Protection Regulation) being the first big move in Europe. Legislation will slowly force companies to ensure themselves better and naturally if you are driving a safer car, then you are generally less exposed to risk.

A Mercedes Benz E Class is just safer than a SsangYong Tivoli.

**Those choosing to try and reap the benefits of the internet also need to try and protect themselves from the drawbacks.** Then it only comes down to how much do you need to protect what you have – and if it is only



# Morten Kjaersgaard

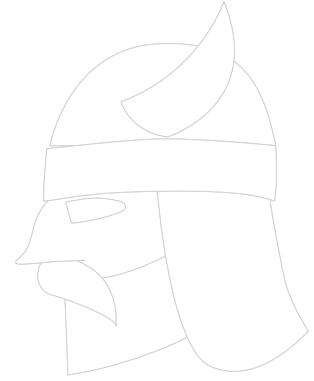
CEO AT HEIMDAL SECURITY 



yourself, then it should be up to yourself, but if you bear the risk of others and you are a payment processor, public entity or similar and therefore hold credit cards, social security numbers and so forth, then of course, then regulation has to be much tougher.

**Taking the global view, the problem will of course be, that the Internet is global and that regulation is not,** hence this possess a global challenge to make the regulation as uniform as possible to make the competitive space as uniform as possible for those trying to provide a service or business within the competitive space.

Internet Security is indeed a battlefield – but I don't think it will ever go either way entirely, but it will improve and evolve over time and



# Morten Kjaersgaard

CEO AT HEIMDAL SECURITY 



eventually the internet will get replaced, the question is just with what and how the security will work there.

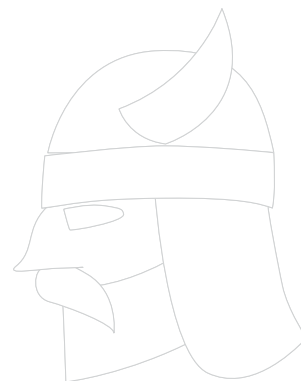
# Can we win the battle against cybercriminals? 30+

#cybersecurity experts share  
their thoughts:



# Neil Kemp

SECURITY CONSULTANT AT NETWORK & SECURITY LIMITED

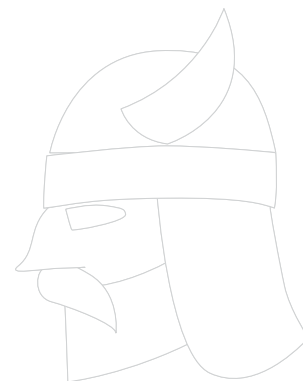


## *Is Internet Security a Losing Battle?*

### **No. It's a War - Not a Battle**

Quite a lot of businesses today approach Internet Security as a one off. Something that can be built and deployed in a couple of months, for example, put in a Firewall, or deploy AV, and then move on to other projects. This can be a blinkered, short-sighted and somewhat risky view. It also should not be considered as an IT issue to be solved, but a Business issue and have oversight, and more importantly buy-in, at Board/Executive level.

Businesses today need to adopt the strategy that Internet Security is one of many Battles in an ongoing War against Cyber Threats and Crime.



# Neil Kemp

SECURITY CONSULTANT AT NETWORK & SECURITY LIMITED



There are new threats and issues that appear every day. Some of these battles will be lost. We advise clients to think as though they have already been breached, not wait until they have been.

## A PROACTIVE SECURITY STRATEGY

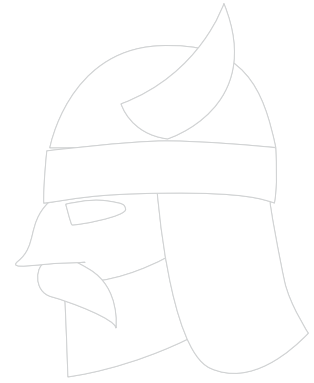
Security Prevention is the best policy. Don't wait until you're hacked or breached to implement elements your Security Strategy. Your business has to act and plan as if a breach has already occurred. This will help you to stay in front. Know your weaknesses, and put in policies and procedures to mitigate any circumstance where it may be exploited as a breach.

Here are some areas you should include in



# Neil Kemp

SECURITY CONSULTANT AT NETWORK & SECURITY LIMITED



your Security Strategy, as a minimum:

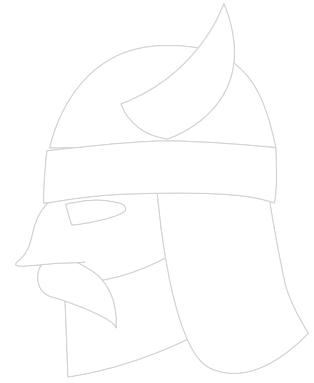
- **Employee Education:** A large percentage of security issues arise from internal issues like a lack of education and knowledge among employees. While you might live and breathe security, employees often don't know the first thing about security.
- **Content Security:** Email & Web – An important vector to secure. Email is responsible for a high percentage of attacks, whether successful or not, a key delivery method for Malware & Ransomware. Where Web security is also key, to develop a policy that can be enforced to prevent infection, access to undesirable sites, misuse of resources etc.

# Neil Kemp

SECURITY CONSULTANT AT NETWORK & SECURITY LIMITED



- **Patch & Vulnerability Management:** Critically, a large number of exploits look for security vulnerabilities in applications. Not only Microsoft but Java, Adobe, etc. should be reviewed on an ongoing basis as well as any third-party applications and services. Also scan regularly for Vulnerabilities – know where your weaknesses are and what to do to mitigate them.
- **Policies:** With these in place, the Business will know what to do and when. Simple, enforced, policies can make the difference between a breach or being secure.
- **Governance and Review:** Make sure your policies are being followed, check and test (and test and test) whenever and wherever you can. Review the threats regularly



# Neil Kemp

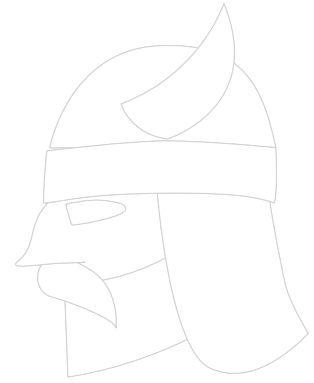
SECURITY CONSULTANT AT NETWORK & SECURITY LIMITED



and update the Security Strategy as needed to adjust for new and emerging threats.

- **Board Level Buy-In:** People at the top need to be informed of what's going on, it's important to get a voice at the top, and budgets allocated. IT Security is a Business problem, not an IT project to be delivered or a problem to be solved.

**Internet security shouldn't be thought of as a losing battle, but an ongoing war.** This the long-term approach will help your organization develop and implement a solid Security Strategy that stands a chance of keeping your Business secure against today's threats.



# Pavel Krčma

CTO AT STICKY PASSWORD



**I don't think that internet security is a losing battle. The battlefield is changing – some battles were lost, some won, but the war continues.**

I think the situation will stay the same until society opens up to accepting broad changes in the way the internet works. For example, the current common principles of full anonymous access and network neutrality don't allow effective filtering of malicious traffic. Additional factors are various government attempts to decrease the security of the whole ecosystem (for example, via forcing vendors to include backdoor encryption access, or by restrictions on the implementation of strong cryptography).

It's like we are somehow stuck in the '80s

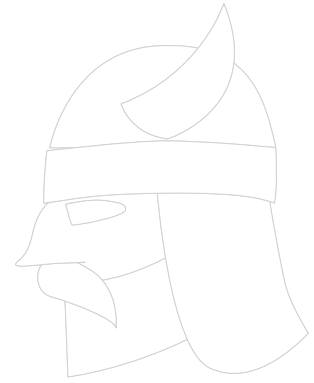


# Pavel Krčma

CTO AT STICKY PASSWORD



when ideas of unlimited access to all internet resources were great. But now, when the internet is global and misuse by zillions of cyber criminals is rampant, it is time to redefine this from a „village of absolute freedom“ to a more real-life tool with common security elements – identification and policy enforcement.



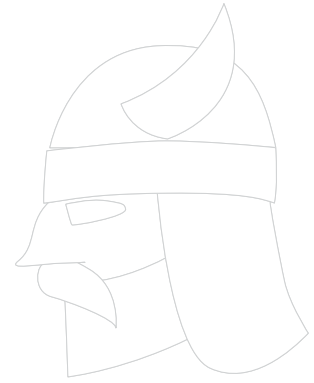
# Peter Kruse

FOUNDER AT CSIS SECURITY GROUP



**First of all, we are not winning. At least not yet. Having said that, neither are we losing.** If we ever win against malicious hackers, vulnerabilities, and malware, then the users, software developers, and service providers need to reflect on what has caused the situation we find ourselves in.

**Let's begin with the end user** – an ordinary internet user still clicking on attachments in emails without thinking first. The end user who is incapable of installing and configuring IoTs correctly and updating them with security patches. The end user who hasn't found out the hard way that failing to patch and update both operating systems and third party products only leads to data loss or financial crime. Perhaps reading a manual from time to time would help, as would stay-



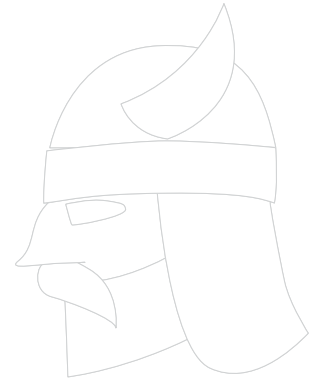
# Peter Kruse

FOUNDER AT CSIS SECURITY GROUP



ing updated on news related to security trends. The end user needs to be better informed to understand the complexity and threats, and how improved internet hygiene can impact life.

**Next, we have the vendors.** *Why are they still so poor at providing truly secure IoT devices that are installed in end users' homes? Most users unwrap their new smart devices, click a few buttons, and hey presto, there we have it: The IoT nightmare. Why not turn the installation of these devices around and force the end user to make security and privacy decisions? Why not start enforcing password changes, or designing services according to installation best practice? Before releasing the product to the masses, why not ensure that the software is written correctly and*



# Peter Kruse

FOUNDER AT CSIS SECURITY GROUP

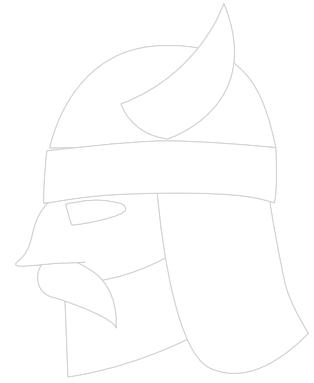


securely by testing it – or have others look and test for vulnerabilities. Additionally, *why not provide updates when needed (preferably installed automatically)*? We have only just begun to see the complications and complexity introduced with these new devices, and those to come.

**Finally, we have service providers in general.** *Why is bulletproof hosting still around? Why not regulate the internet?* Bad net blocks should be reassigned or cut loose if the owner is either constantly breaking the rules or not preventing attacks from hitting innocent internet users and networks.

**We should perhaps rethink how we could cleanse all the bad stuff, and arrest IT criminals in a more coordinated and efficient**





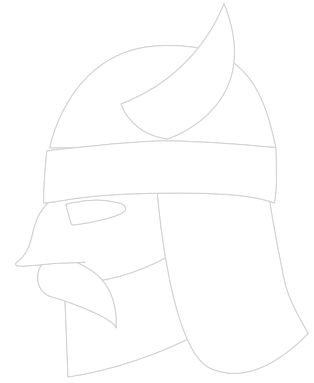
# Peter Kruse

FOUNDER AT CSIS SECURITY GROUP



**way.** I know this has been discussed for decades – and there really doesn't seem to be an obvious solution – but if we strive to win, then end users, vendors and service providers need to learn, to improve and to become more efficient at catching and breaking criminal services.

**No, we haven't lost yet. But to win, we certainly need to improve.**



# Pierluigi Paganini

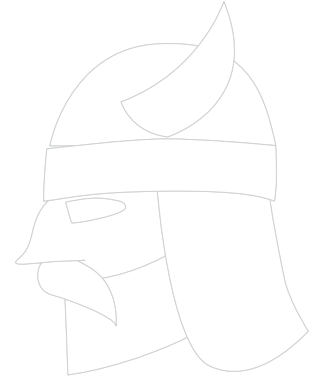
CIO AT BIT4LD, MEMBER OF ENISA & FOUNDER OF SECURITY AFFAIRS



First of all, we have to contextualize the discussion. We are assisting to a rapid increase of cyber threats and of their level of sophistication. Technology like Internet of Things is dramatically increasing our surface of attack, and unfortunately, there is still a low perception of cyber threats among populations.

If you think of the Internet such as a “global commodity,” you cannot forget that it was not designed to be resilient to cyber threats. This means that its backbone should be re-designed with this specific focus.

What we can do in this historic phase is start spreading a security by design approach for every connected object that could be abused by threat actors.



# Pierluigi Paganini

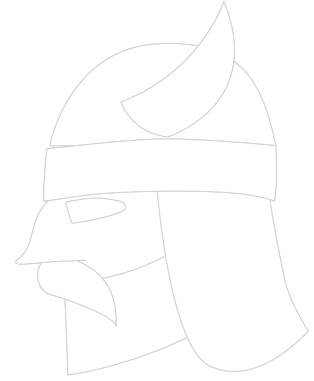
CIO AT [BIT4LD](#), MEMBER OF ENISA & FOUNDER OF SECURITY AFFAIRS



**We urge more information sharing on cyber threats and we need a global acceptance of shared norms of state behavior to prevent both governments and non-nation-state actors of harming the Internet.**

# Raul Popa

CEO AND DATA SCIENTIST AT TYPINGDNA 



I think Internet security is a large category and there are lots of security measures that work, others that do not, but **it's not a losing battle altogether**. Some things are broken and need to be fixed, others are broken by concept and can't be patched perfectly. Obviously, there is a huge market for both security software and hacking in the latter.

The Internet, as a whole hasn't been designed for what it is today, it evolved this way, and there are hundreds of cracks that can be exploited all over it.

Typically, there are 3 major types of frauds and security issues by the point of attack: client (endpoint), connection and server.

First thing: everybody should fix their con-



# Raul Popa

CEO AND DATA SCIENTIST AT TYPINGDNA 



nection, use a firewall, use https, email should be secured, LAN should be careful setup, WIFI should be protected. There are a few simple tricks and your connection could be hardened to an ultra high potential.

Secondly, if you're in the software business, if you have a website, or an app: the server part is as easy to secure, and with the rise of cloud computing, all major players are taking care of most of your stuff. If you're big enough get a specialist to help you with security or at least pay a security firm to audit and do a penetration test for your apps. Ethical hackers may help you too.

However, **the biggest problem is the user.** People are using very simple passwords, they don't use 2nd-factor authentication,



# Raul Popa

CEO AND DATA SCIENTIST AT TYPINGDNA 

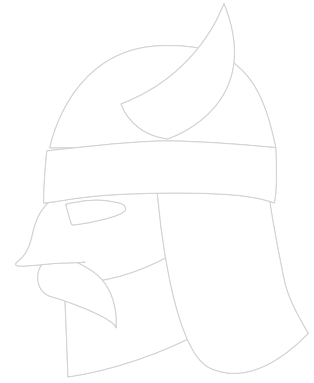


they share accounts, they open phishing emails, they click on suspicious links, they leave their PCs unattended and unlocked, and the list may continue. **But the real problem is that people don't know how to protect themselves and that they don't care.** I'm not saying that system exploits are not around anymore, they still haunt us all, but technically if your computers are up to date, you're at lower risk from a pure technical exploit and that's pretty much all you can do about it.

**Hacking nowadays is focused more and more on exploiting human vulnerabilities,** on social engineering, or at least on combinations between phishing/viruses and human interaction. Experts found out that it is harder to scale exploits based on system

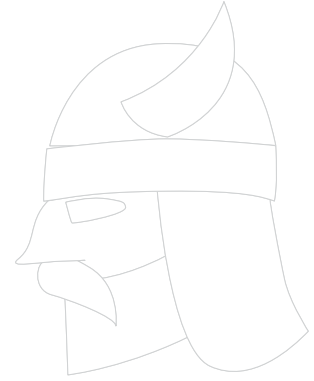
# Raul Popa

CEO AND DATA SCIENTIST AT TYPINGDNA 



vulnerabilities alone and they can do little damage. “Luckily” there are social engineering techniques that work at scale especially when combined with basic system exploits.

Let’s take phishing for example: in it’s simplest form, a user gets an email from someone who looks like a friend, coworker, or simply clicks on a link on some “grey-zone” page, an exploit is installed on his PC which typically starts gathering passwords, credit cards, and other interesting information. Once you have access to people’s passwords it’s easier to get to their money, and that’s how basic cybercrime and online identity theft works. In the corporate world, the problem is even more complex, as people care even less about the company data and they don’t follow security procedures.



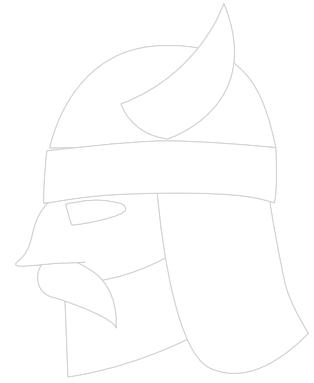
# Raul Popa

CEO AND DATA SCIENTIST AT TYPINGDNA 



So, in order to harden Internet security, it's important to understand how attacks work, protect user accounts from the apps, implement 2nd-factor authentication everywhere and protect browsers, PCs, phones and (now) IoT devices stronger than ever before.





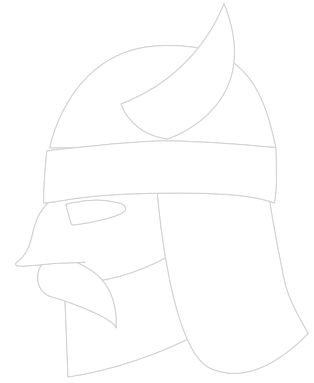
# Ryan J. Corey

CO-FOUNDER AT CYBRARY



**I don't necessarily think that internet security is a losing battle in the long run, but I do believe it will get worse before it gets better.** One thing we can count on is that the bad actors are working hard to make their attacks more mature all the time. For the users, despite the chatter about security awareness, too few companies are adhering to a practice that informs their employees about the latest forms of attacks. Also, the technology has a way to go, there really is no one tried and true solution that is infallible. Until more of the everyday internet users become aware, and easy full-scope solutions become commonplace, I believe the landscape will become slightly worse.

In regards to the long term, I believe things will get much better in internet security. We



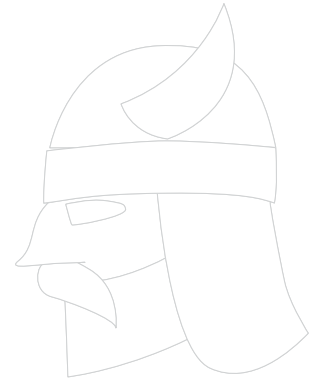
# Ryan J. Corey

CO-FOUNDER AT CYBRARY



have really only been truly facing the issue for less than a decade. More exposure is driving attention to the concept of awareness, and momentum seems to head in the right direction for that, despite its relatively low saturation among all users. Furthermore, venture capitalists are pouring a lot of money into cybersecurity innovators, and we have seen huge leaps in the tech in the last couple of years. So I do believe, eventually, we will come to a point where the world can breathe a little easier when it comes to internet security.

# Sergiu Sechel



SENIOR ADVISOR – IT ADVISORY SERVICES AT EY



*Is Internet security a losing battle?* It is a difficult question and I don't believe that there is a definitive answer to it. Mainly because this "Internet" in 2016 is like a galaxy of interconnected networks made up of computers, mobile devices, smart peripherals, network devices, IoT devices, industrial control systems, smart cars and so on. This "Internet" we are trying to secure provides just a set of communication protocols so that all the connected devices can talk to each other and exchange data. It is true that the TCP/IP protocol stack that enables all this plethora of devices to connect to the Internet it is a bit old, and some of the protocols like DNS and BGP, for example, need to be updated, but in general the Internet protocols, configured correctly are secure. Also, the adoption of the IPv6 protocol (which is slow) will



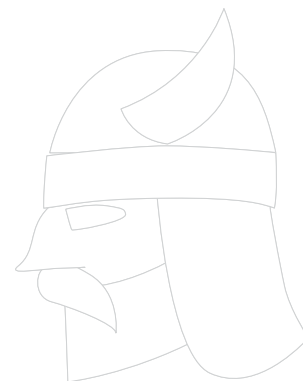
## Sergiu Sechel

SENIOR ADVISOR – IT ADVISORY SERVICES AT EY



secure the Internet communications better than IPv4 mainly because IPv6 has the IPsec encryption stack embedded in by default.

People reading the opinions given above will argue that just last month the Internet in North America was almost shut down on Oct 21st after a distributed denial-of-service (DDoS) attack on the DNS provider Dyn. It is a true argument but the Mirai botnet used in the attack that generated almost 1TB/s of legitimate traffic was possible because of poor security configuration of millions of IoT devices because after deployment the users never changed the default passwords. A similar attack involving a Mirai botnet denied Internet access to the country of Liberia in early Nov 2016. **Internet security is**



# Sergiu Sechel

SENIOR ADVISOR – IT ADVISORY SERVICES AT EY



**as strong as the security of the interconnected devices that make up the Internet.**

Coming back to the question “Is Internet security a losing battle?”. I don’t think so, **I believe it is an ongoing and evolving battle**, and since it’s inception the Internet has only gotten more secure over time. After the dot-com bubble (1995 – 2001) from 1999 until 2009, there were some important virus outbreaks that forced the IT industry to rethink cybersecurity. Some can remember the most famous viruses in the 2000’s:

- Melissa(1999) (~1,2bn USD in damages);
- ILOVEYOU(2000) (~15bn USD in damages);
- Code Red(2001) (~2bn USD in damag-

# Sergiu Sechel

SENIOR ADVISOR – IT ADVISORY SERVICES AT EY



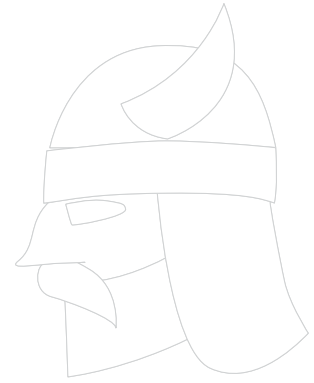
es);

- Nimda(2001) (~635mn USD in damages);
- Sapphire(2003) (~750mn USD in damages);
- Sasser(2004) (~500mn USD in damages);
- MyDoom(2004) (~38bn USD in damages);
- Conficker(2008) (~9.1bn USD in damages).

**In total, these 8 virus outbreaks caused ~67,18 billion USD worth of damages in the span of 10 years.** The industry responded to each of these threats and mitigated the vulnerabilities that enabled the outbreaks to occur, making the internet safer.

# Sergiu Sechel

SENIOR ADVISOR – IT ADVISORY SERVICES AT EY

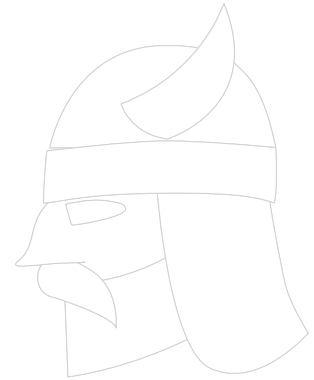


After that period, the mobile revolution started and businesses and users started to bring parts of their life on the internet and vice-versa. At the same time, new threats, like the banking trojans, APT's and cyber war appeared and they are still ongoing threats today. In the last 3 years, threats to our privacy in the form of mass surveillance made us reconsider how much of our lives we should share on the internet and how to protect the things that we choose to share.

Now we are talking about exciting technologies that are possible thanks to the internet, like autonomous traveling, IoT, blockchain and distributed ledgers, technologies that promise to disrupt, redefine and reshape our social lives and they are dependent on the internet in order to work. All of them come

# Sergiu Sechel

SENIOR ADVISOR – IT ADVISORY SERVICES AT EY



with great promises, great benefits but they also bring bigger risks from a cyber security perspective.

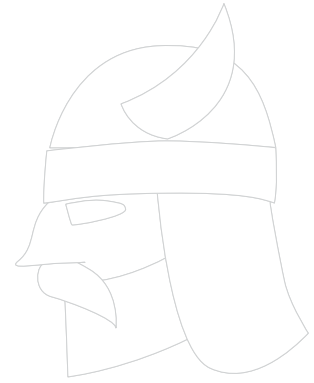
***How can we change the internet security from a losing battle to a winning battle?***

**Companies, governments, people need to invest time and resources in cybersecurity education.** As teenagers and students learn in schools and colleges how to code, sufficient time should be dedicated to teaching them secure coding principles and practices. **The general population needs some basic training on cyber security.** If the users that deployed those IoT devices took 1 minute of their time to change the default passwords on their devices they would have individually stopped an attack that in the



# Sergiu Sechel

SENIOR ADVISOR – IT ADVISORY SERVICES AT EY



end managed to impact them collectively.

Companies and governments need to invest time and resources to train their IT personnel and their security personnel. Technologies are evolving at a fast pace and threats are evolving as fast. IT personnel training should keep the pace with the challenges posed by new technologies and evolving threats. Studies performed by ISC2 and ISACA show that the demand for cyber security personnel will reach 6 million globally by 2019, and they forecast that the supply will be around ~4,2 million in skilled cybersecurity professionals available globally by 2019.

# Stan Hanks

CHIEF TECHNOLOGIST AT COLUMBIA VENTURES CORP



## We're Doing This All Wrong

I've been working in network security since the early 1980s, have been a proponent of much of what has come to be accepted as "best practices" and regrettably, have come to accept in recent months that we're just doing this all wrong. And sadly, it's not that we are doing things poorly, rather we're just doing the wrong things.

Let's look at the history of keeping secrets and managing confidential information. For a tremendously long time – from around 3200BCE in Mesopotamia until probably sometime in the 1960s, information existed only either as ideas in someone's head or as a written document.

# Stan Hanks

CHIEF TECHNOLOGIST AT COLUMBIA VENTURES CORP



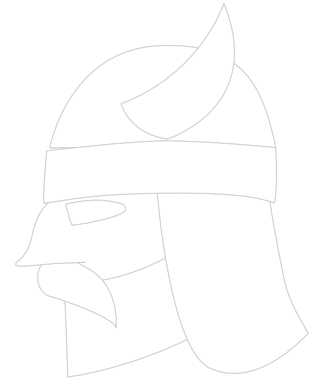
All of what we think of as “information security” has its roots in this – the management of physical documents. If you are allowed access, there’s not only a protocol for physically gaining access, but for preventing others from gaining access while it’s in your custody, and for auditing that whole path. And there are guys with weapons scurrying around to ensure that you both don’t violate the policies and to intercede if you do.

That worked really pretty well, until the advent of xerographic copiers; at that point, the rules were modified a bit but remained essentially the same: physical access is the golden rule. Control physical access, you control knowledge.

By the mid-80s, when it became clear that

# Stan Hanks

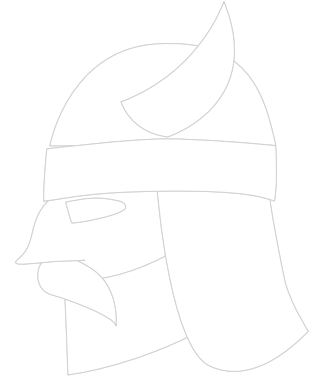
CHIEF TECHNOLOGIST AT COLUMBIA VENTURES CORP



networks were going to be a thing and that computers were going to be ubiquitous, the US Department of Defense issued a document known as “The Trusted Computer System Evaluation Criteria”, known as “The Orange Book”, which became the go-to document for much of what has transpired since then. And that’s largely the problem.

The Orange Book was written for a military audience and was a translation of practices around handling paper documents. All of the underlying models are based on physical access models carried over from the management of paper documents.

Even our use of passwords is closely related to the standard issue Sargent and Greenleaf the position non-manipulative locks used to



# Stan Hanks

CHIEF TECHNOLOGIST AT COLUMBIA VENTURES CORP



secure filing systems in the military. You can't re-use old ones, you are forced to pick new combinations on a regular basis, and God help you if you forget what you chose...

Yet, here we are in well into the 2000s, espousing the same theories. And it's just wrong. It's based on a military model that doesn't apply to civilian audiences. It places a burden – a seriously undue and unconscionable onerous burden – on the user. You know, *the user? The person who is actually PAYING for us to do all of this stuff? The person who we should be catering to in the extreme?*

The nature of the problem in managing digital information is hugely different. The information isn't just the result of an individual



# Stan Hanks

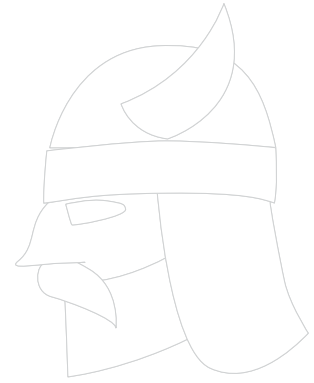
CHIEF TECHNOLOGIST AT COLUMBIA VENTURES CORP



creating a document; the information creates itself, from actions taken ranging from visiting websites to downloading apps on a phone to playing games in particularly locations to just simply walking around with a location-aware application running in the background.

That's... not the model. The model is based on something different, something more tangible, something less voluminous.

And as the data has grown, so have the number of use cases in which security is important. In the 1980s, when the Orange Book was developed, it was typically the expected case for the user to have one account on one computing system. Today, I've got probably close to a hundred accounts on



# Stan Hanks

CHIEF TECHNOLOGIST AT COLUMBIA VENTURES CORP

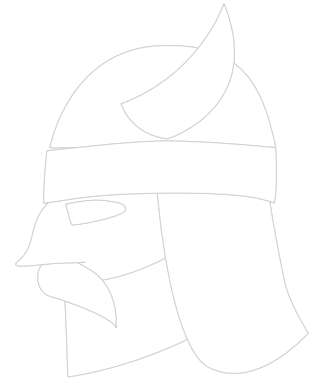


a variety of platforms from embedded devices to email to public forms and beyond.

All of these platforms have the same broken security mechanics, based in large part on the models from the earliest time-sharing systems, or more particularly, UNIX.

There have been advances in areas such as biometrics, and multi-factor authentication and the like, but the roots are the same: deep, deep down in the core of the system, it KNOWS that it's managing documents and that it's the only system that you use, and that managing passwords is not a problem, because you only have the one.

That's just broken. We need to stop it. We need to stop creating systems which force



# Stan Hanks

CHIEF TECHNOLOGIST AT COLUMBIA VENTURES CORP



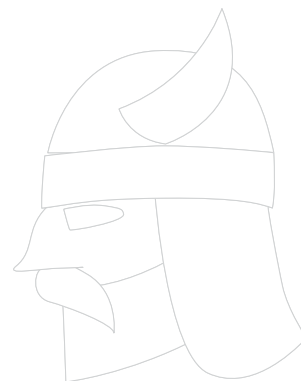
the difficult and painful use factors onto the users and rather pull them into the core of the systems where it actually does the most good, and in doing so, create seamless and effortless authentication systems for users. Systems not easily broken. Systems not subject to social engineering attacks. Systems which don't induce use of little sticky notes to "remember" the password you were forced to change at gunpoint, as it were.

I don't know what the answer is – yet. But I'm sure it's not "beefing up" what we already have, because if that were going to work, it would have worked by now.



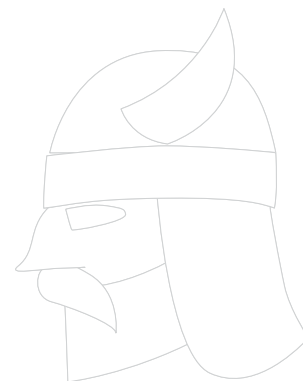
# Stefan Tănase

SENIOR SECURITY RESEARCHER AT  
KASPERSKY LAB GLOBAL RESEARCH & ANALYSIS TEAM



**Internet security is more like an ongoing battle than a losing battle.** It's not something you "own" and then you go on living happily ever after. Or it might be a losing battle from the very beginning, only if you expect a security solution to offer 100% protection. There is no such thing and whoever says there is, is not telling the truth.

However, security solutions do offer reliable protection for private users and companies but additional measures are required. Installing all necessary updates, backing up important files and not trusting anyone are equally important. Also, becoming more cyber-savvy about the online environment and the threats they might face on the Internet is highly recommended for private users.



# Stefan Tănase

SENIOR SECURITY RESEARCHER AT  
KASPERSKY LAB GLOBAL RESEARCH & ANALYSIS TEAM

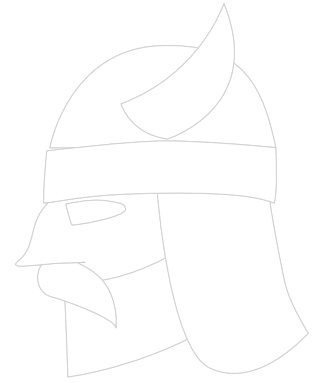


Businesses too need to change their approach. The growing complexity of their infrastructure, the lack of security intelligence, as well as the continuously changing threat landscape – all these are reasons strong enough to change the good old way when a security company could just deliver a product license key and come back one year later for renewal. This is not working anymore.

**Although it would be easier for everybody – security companies and businesses – there is no “one solution to solve each problem”.** Security is a process and I think the service model is the best way to deal with it: from security audits to training sessions for employees and predicting future attacks based on threat intelligence, it is a very complex

# Stefan Tănase

SENIOR SECURITY RESEARCHER AT  
KASPERSKY LAB GLOBAL RESEARCH & ANALYSIS TEAM

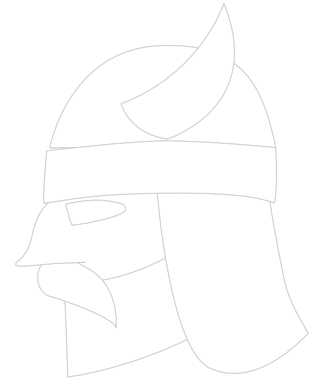


model. But it works for both enterprises as well as small companies that could become victims of attackers who target large companies.

**Last, but not least, one more thought on Internet security: you can achieve it without having to fight for it only when the cost of an attack exceeds the value of the data obtained as a result of that attack.**

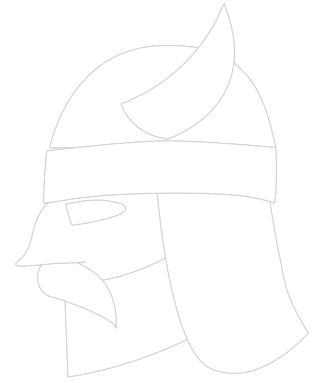
# Tony Perez

CEO AT SUCURI SECURITY



Of course not! That's like saying: well there is crime, let's just do away with law enforcement.

The security challenges that the internet presents us today are similar in nature to the security challenges we've faced over the years in a number of industries. Take the Microsoft OS into consideration, look at how they've evolved over time. Today they have some of the more security by default configurations you've seen in any OS. This comes from years and years of trials and tribulations, had they stopped, *where would the world be without the Windows OS?* (Some might argue in a better place... hehe.) Another example is WordPress, look at where they are today, relative to where they were 13 years ago. They too have adopted a security



# Tony Perez

CEO AT SUCURI SECURITY

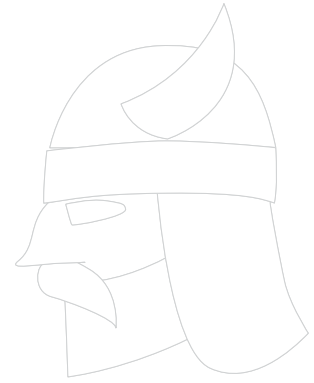


by default configuration, and in the process, we've seen huge improvements (relatively speaking) to the impacts of websites getting hacked.

There is no denying however that we do find ourselves in a precarious position today with the state of internet security. Security was not part of the framework when the various bits and pieces were meshed together to create what we recognize today as the Internet. Just look at the past 5 years and the number of issues that have been disclosed in technologies that were considered to be relatively stable. Now introduce this desire for everything to be interconnected, the demand by the population to have readily accessible data at all times, the inclusion of IoT devices and we find ourselves with a

# Tony Perez

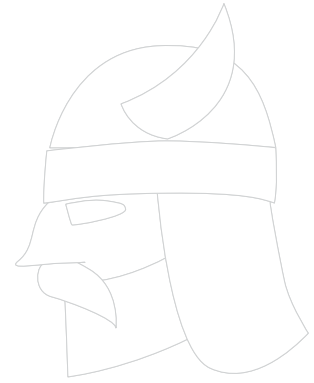
CEO AT SUCURI SECURITY



recipe for disaster.

We've already started to see some of the challenges this introduces. We've seen critical infrastructure for nations be attacked, successfully. We've seen the backbone of the major internet providers attacked. We've seen censorship of reporters and voices around the world. It's definitely not a pretty picture, and I fear that we haven't fully grasped the full potential of today's security threats.

With that being said, **I would never give up or say that we're at such a point that we should throw our hands in the air. Instead, I would challenge the security community to be more inclusive and learn to better collaborate with one another.** I think there is some-



# Tony Perez

CEO AT SUCURI SECURITY



thing to be said for how open-source technologies work, and as industries, we can learn a lot. Interesting enough, the greatest challenge I see is not the security threats, but rather the commercialization of the industry and what that entails. What's funny is that in the trenches, most of the researchers are willing and open to collaborating with another to solve some of the biggest problems, they don't publicly though because of management and bureaucracy. It's not that we're not able to combat today's challenges, it's that we're not willing.

# Conclusion

I hope you've enjoyed reading this roundup and kudos for making it this far (this is the lengthiest article on our blog so far)!

A big **thank you** for all the experts who lent their time and experience so that we can all get better at our own cyber security.

The fight against cybercrime continues and I hope these perspectives will help you better choose your protective "weapons" and arm yourself with the right knowledge going forward!





# HEIMDAL

## SECURITY

**We protect users and companies from cyber-criminal actions, by keeping confidential information and intellectual property safe.**

As cyber-criminal attacks increased and data leakage became a major issue for every individual and every organization, there appeared a growing demand for a security solution to ensure that confidential information never leaks to a hacker controlled server.

The Heimdal Security software was developed in 2011 by the 19th and 20th Team Defcon CTF World Champions in hacking. Heimdal is now used to protect organizations across Europe against advanced attacks, wherever their users may go.

That's why our product has been created to address the real-world need for a solution against cyber-criminal actions and their malicious tools. For these reasons, we are recognized in the online community as fighters against hackers and their malicious actions.