CYBERSECURITY FUNDAMENTALS

RISKS, PROCEDURES, & INTEGRATION

MEDIA PLANET Future of Business and Tech

Table of Contents

Weak Systems, Strong Attackers: Cyber Security in the Modern Age

The 2015 Annual Report from the Pentagon acknowledges that most military cyber systems are vulnerable to "low to middling level" cyber attacks, and most DoD operations can be compromised when and if the attackers choose to do so.

If the most sophisticated, and best-funded, military operation in the world can be compromised by "mid to low level" cyber attacks, how secure can we reasonably expect discount retailers, movie studios or any other organization to be?

The bad news

The core system of the Internet is actually getting weaker as we connect ever more of our lives—phones, tablets, cars, refrigerators—to it.

Meanwhile, the attackers are getting stronger. The sophisticated attacks we saw only between nation states a few years ago are now being used by common criminals against all sectors of the economy. And they are not just after credit

cards. Intellectual property, health records, business plans, and trading algorithms—anything of value is at risk. Modern attackers typically compromise your system and then hide, periodically turning themselves on to phone home with your stolen data.

> "The sophisticated attacks we saw only between nation states a few years ago are now being used by common criminals against all sectors of the economy."

Finally, the economics of cyber security favor the attackers. Cyber attack methods are relatively cheap, easy to acquire and profit margins are enormous. Defense is hard after the fact, and there is almost no law enforcement. We successfully prosecute maybe 2 percent of cyber criminals.

Better defenses

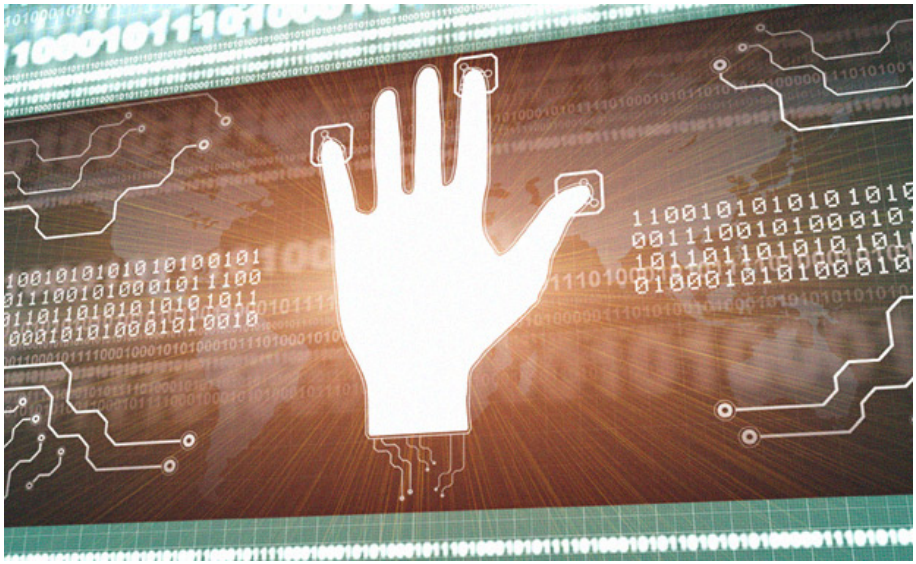
In this environment, the notion of perimeter defense is antiquated. Businesses need to rethink their approach to cyber security focusing less on breaches and more toward developing a comprehensive cyber-sensitive business strategy.

A useful analogy is personal health. No one expects to live germ-free. However, by practicing good basic health rules, we can fight off most of the germs that attack us. Still, at some point we all get sick and we need to know how to recover when we do and get ourselves back to full health as soon as possible.

Key to this approach is integrating cyber security into the everyday business decisions. Much like legal and financial issues in the modern world, virtually every business decision—including product development, vendor and customer management, M & A, human resources—all have cyber security dimensions.

Wise enterprises follow good cyber hygiene and integrate these principles throughout their business while devoting special attention to their most critical data. They also have practiced plans for when they are successfully attacked so they can retain their resiliency and continue to grow and prosper.

Anatomy of a Cyber Crime



Who is this community of cyber criminals? And what organizations exist to counter this growing threat?

Leading the charge

The ISSA (The Information Systems Security Association), a non-profit organization that provides community– based education, awareness and training in effectively managing cyber crime and the President of its Los Angeles chapter, Stan Stahl—one of the country's leading experts on cyber security—are at the forefront of a movement that is closing the gap between the people with the means and motivation to commit these crimes, and both their victims and the law.

> "Like Tony Soprano, there are bosses," says Stahl, "but instead of sending out their goons, these guys have their geeks."

Cyber crime is in many ways the natural evolution of any other kind of organized crime, and the criminals run their operations in a similar way. "Like Tony Soprano, there are bosses," says Stahl, "but instead of sending out their goons,

these guys have their geeks," highly specialized experts who look for and exploit vulnerabilities in the code of commonly used programs. Cyber crime is a global industry. "For example, a cyber-criminal in the Ukraine is planning a job where money will need to be transferred out of the country. He will call up a buddy in China and say 'I need 80 money mules to move $700,000 next week.'" Cyber crime is, "run like a business," and it is becoming big business.

Behind the mask

Where there is a will there is a way, "and the way," says Stahl, "is like shooting fish in a barrel, because businesses are woefully unprepared." The creativity of the cybercriminal in terms of how to monetize information is virtually limitless. "If you can imagine it, it can happen," everything from stealing people's identities, medical insurance to, "honest to goodness dollars from the bank accounts of businesses," says Stahl, "and what's worse is that when the company that's been victimized calls their bank, the bank is not obligated by law to give the money back."

According to Stahl, a big part of the problem is a denial of how serious the problem is, but "a critical piece of the solution requires that businesses, banks, information systems security professionals, and associations like the ISSA, all get involved and come to the table and deal with this issue in a way that's practical and workable. So much could be done just by sharing information and the collective wisdom of the community." Having a conversation among the right people is the first step in building a community that is able to effectively defend itself from today's cyber criminal.

How to Work Around the Inherent Flaw of Cybersecurity

What I'm about to say may sound a bit heretical, given my profession as a cybersecurity attorney, but for many years we have been living with the myth that we can completely protect our computing systems from cyberattacks. Although preventative measures can help reduce the likelihood of a breach, most people in the cybersecurity industry know a dirty little secret: You can never keep the cyberattackers out.

Raising the "price" for hackers

In 1964, internet pioneer Paul Baran from RAND said we must presume that the attackers have already penetrated our ostensibly secure systems. His solution in 1964 was to "raise the price of the espied system to a point where it becomes excessive." This still holds true today.

Put another way, we need to make our computing systems more expensive to attack successfully and, therefore, less attractive to the cyberattackers. This is because the cyberattackers only need to be right once. In contrast, you theoretically need to be right every time whether you are a large multinational corporation, a small-to-medium business, or an individual or home user. The myth of cybersecurity is that stopping 100 percent of cyberattacks can be achieved.

How to plan ahead

Pundits debunking this myth have begun to hit the mainstream. A popular phrase (actually attributed to the Director of the FBI, Robert Mueller) states that there are two types of companies, those that know that they've been hacked and those that just haven't found out yet.

> "The myth of cybersecurity is that stopping 100 percent of cyberattacks can be achieved."

What this means is that all stakeholders need to put in place a combination of proactive and reactive planning measures in order to "raise the price of the espied information" prior to a successful cyberattack, and then have a plan in place after a cyberattack has occurred. If each stakeholder accomplished this, we could eliminate the majority of common vulnerabilities and cut down significantly on successful attacks.

Tactics for businesses and individuals

Although many expert lists of "best practices" exist, the two lists below outline a few things that both businesses and individuals should consider to eliminate being easy targets. Trust me, these may sound like common sense, but you would be amazed at the number of situations that we deal with on a daily basis that could have been prevented by these relatively straightforward tactics.

Top five actions that an enterprise should consider include:

- **Start strong.** Create a security and privacy governance structure, such that

your entity is secure by design.

- **Stay vigilant.** Research threats to the organization and perform a risk analysis on those threats.
- **Make a list.** Prioritize the information assets of the organization.
- **Formalize your process.** Create a security protection plan that is tied to a technology acquisition strategy.
- **Ask for help.** Utilize third parties that have been appropriately engaged, including legal and technical personnel (or contractors).

Top five actions that an individual should consider—both for personal security and to protect their employer or any organizations with which they are affiliated:

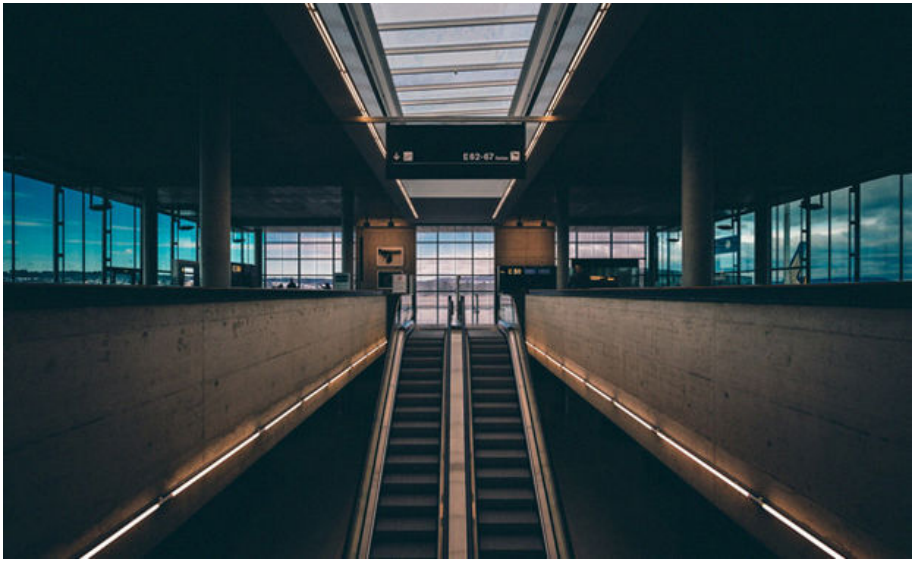
- **Anticipate.** Be aware of the consequences to which your actions could lead. If you post personal information for public view, be aware of the results.
- **Guard your cursor.** Don't click on something that doesn't seem quite right. Phishing (emails sent to massive numbers of people containing malicious payload) and spearphishing (same as phishing, but cleverly disguised to look like a real email by being directed to a specific person and containing realistic-looking content) both rely on people clicking on links or opening emails and attachments that contain malware. If you get an email from someone you don't know or that you didn't expect, call the person first.
- **Switch it up.** Use a different strong password for each site where you will be transacting financial business or sharing sensitive information.
- **Back up your data.** Without data backups, you could wind up being victim of ransomware or some other attack that destroys or makes unusable your current data.
- **Refresh your system.** Make sure your computer defenses are operating and up to date.

An optimistic outlook

While things may seem bad based on the constant barrage of stories about data breaches, ransomware and phishing attacks, the collaborative efforts of all stakeholders can create an environment where the cyberattackers cannot easily breach our defenses. When they do attack (and they will), having a plan in place to deal with the attack will go a long way toward minimizing the damages.

With the cooperation of the government and the private sector, in combination with the diligent efforts of all citizens, we can increase the effort required by the attackers to penetrate our systems. Once we do that, we will significantly reduce the exposure of our systems. Or, as Paul Baran would have said, we will have raised the price of the espied information in a way that causes the attacker to go somewhere else.

5 Ways to Protect Your Business from Cyberattacks



As a result, a major focus has been on risk mitigation and response plans for cyberattacks, security breaches and the like.

Fundamentals matter

Organizational educational programming and process improvements have focused primarily on defensive positioning against these technological attacks, which could enable your internal plans and information to get into the wrong hands and jeopardize your competitive advantage. We go on the defense with extensive education and advice about selecting passwords, locking phones and computers and so on, that we get very careless about all of the other ways hackers find out what your organization is doing.

Traditional ways of gathering competitive information have been forgotten by companies in the age of technology and cyberattacks. Don’t get me wrong,

mitigating cyberattacks is of utmost importance. But don't forget the basics of practical counterintelligence education that should be part of every employee orientation, certification or refresher course, so employees are not inadvertently giving away company secrets.

> "Traditional ways of gathering competitive information have been forgotten by companies in the age of technology and cyberattacks."

What to ask

The startling truth is that most organizations don't even know they are vulnerable and incorrectly answer these questions. How much can your competitor learn about your company from public information? How informed are your employees about information sharing? How is information unintentionally leaked and how significant is it? How do "information hackers" use bits and pieces of information to build a picture of you or your organization?

If you don't have clear answers or a mitigation plan to eliminate risks associated these questions, then your organization is likely vulnerable even with the best technologies, firewalls and security software, because these threats are not happening in cyberspace.

They are happening in airports when your leading sales representative is waiting to board a plane, discussing the large deal he or he just closed for X number at Y price. Compromises are happening when R&D scientists are discussing the new war ship radar system during a breakfast at the hotel down the street from X company's innovation lab in Washington DC. They are happening on the commuter train when the consultant is preparing the final recommendations presentation for tomorrow's meeting.

Risks and fixes

Secrets are passed on in the most obvious but least expected ways, and they are used by trained experts to build a solid picture of your company plans. So why do we fail here?

So, here are five steps to tighten up the leaks:

1. Stress test

Conduct a full countermeasures vulnerabilities assessment of your company.

2. Emergency plan

Develop a quick response plan to recognize and address threats.

3. Priority pages

Recognize NDAs and Conflict of Interest agreements only protect your organization in limited fashion. Most employees don’t give away information on purpose.

4. Orientation

Educate all employees in countermeasures and make it part of their orientation program.

5. Word of mouth

Remind by recertifying resources: post signs, brief before sales meetings or trade shows in order to remind employees and retrain periodically.

Robert Herjavec's Advice for Navigating Cyberattacks

What motivated you to enter the cybersecurity space in the first place?

Robert Herjavec: I've been in this business for over 30 years. I entered the IT space because I was waiting tables and needed a better job. My friend was passing up the opportunity for an interview with a computer company and, when I learned how much it paid, I jumped at the chance to get in there and be interviewed.

Once I started in the IT business my love for it grew almost immediately. I was blown away by how quickly things changed and by what technology was capable of. Think back to the tech of three decades ago: We're talking the first ethernet connections. I remember the early days of Herjavec Group when our sales team's first question on a cold call to a customer was, "Do you have an internet connection?" If yes, they'd ask more questions, if no they would say thank you and hang up. We don't have that problem anymore.

How has the industry changed since you first became involved?

In 2003 we recognized that enterprise organizations needed to keep their data secure, but in some ways we were ahead of the curve in our offering of services. We offer consulting, delivery, managed services and remediation support to large-scale organizations with very complex environments. We really couldn't have predicted how far our space would come in such a short period of time. If I look back 30 years—wow—entirely different.

The internet, cellular phones, the proliferation of technology, Internet of Things. It's all about interconnectivity today and the key word is "more"—more endpoints, more connections, more data, more threats, more risks. Today when you walk through Times Square in New York, the billboards can track you via your mobile phone and you'll receive spot advertising customized for you. That's incredible to me.

Yes, today it's digital marketing 101. But think of all the pieces of technology that have to integrate to make that possible. Also think of the risks; cybersecurity is mainstream today because we've seen the repercussions personally, professionally and financially from not keeping our corporate and customer data secure. Security isn't an IT issue; it's a board-level issue for organizations globally. To speak more broadly, it's a global citizen issue. The wars of today and even tomorrow will continue to play out via cyber warfare.

How does your team at the Herjavec Group continually evolve in order to stay ahead of hackers along with the threats they pose?

One of the key ways we stay ahead is that we employ a team of ethical hackers on our consulting team. Their job is to leverage the latest hacking techniques in order to assess the security postures of our clients. We also partner with best of breed technology providers globally to ensure we're bringing emerging technology to our customers. We have to learn from each other so it's important we understand the latest technology, have the ability to architect and configure it and then can develop services to support it. That's how we stay ahead of the curve and proactively defend our customers from the latest cyberattacks.

What is an emerging trend or initiative within the cybersecurity industry that really excites you? What keeps you up at night?

Proactive threat detection and investigation is becoming the norm. It's no longer

ok to just block and defend. The role of the Threat Hunter is becoming pivotal as we're seeing the growing need to detect, investigate and analyze very sophisticated and persistent threats in large organizations. Organizations want to know where the threat originated, how they should respond and what can be done to contain the incident.

More and more, our customers are seeking answers to the risks out there in the deep dark web and we need skilled professionals, Threat Hunters, to support that level of work. What keeps me up at night? I'd say paranoia. I firmly believe only the paranoid survive. Jamie Dimon, CEO of JP Morgan Chase, said it best. He doesn't stay up at night worrying about the markets; he's worried about a cyberattack. You should always be worried about what you don't know and in my line of work, you've got to be paranoid.

What's a realistic goal for the industry to strive for this coming decade? What's a stretch-goal we should be pushing for?

I'd love to see our industry focus on educating the youth of today about cybersecurity risks and information security in general. We have a shortage of talent and training in this sector that needs to be resolved because the risks we are facing aren't going to decrease over the next 5 to 10 years. We need the support of post-secondary institutions to help teach a new generation of students how this technology fundamentally works so we can have a greater talent pool to pull from.

I've given so many speeches where I call out the 0.0 percent unemployment rate in security. It sounds insane given today's economy, but it's true. Cybersecurity professionals are highly sought after and we need to ensure we're replenishing the talent and teaching the next generation.

On Careers in Cybersecurity

To get a better grip on the gap in the cybersecurity workforce, we checked in with Christopher Casale, a recent M.S. graduate fom the University of South Florida student about his path to cybersecurity and what he'd recommend aspiring professionals look for in a program.

What motivated you to pursue a major in cybersecurity or information assurance?

I started my career as a software developer almost 20 years ago, before transitioning into leading teams of developers. It's been interesting to see how the questions have changed over that span of time. When I first started, companies were concerned with what features they would build into their software. Eventually, those concerns shifted into user experience and how customers would interact with the software.

For the last 5-plus years, the questions have been about security. How can we keep the information safe, how do we know it's safe, and how do we balance convenience with security? I decided to pursue an M.S. in Cybersecurity with a focus on information assurance so I could better understand and answer those questions from the beginning of the Software Development Lifecycle through delivery.

What advice would you give to prospective students looking to major in this field?

This isn't the type of field where you can read it in a book, memorize it and write it down on a test, so be prepared to work. It's not only about understanding the concepts, but how they're applied in real-world applications. This should be reflected in the type of program you select. The best programs include a good amount of hands-on experience and projects as part of the curriculum.

I would also recommend a basic understanding of coding. You don't necessarily need to be a programmer, but knowing how to write basic shell scripts will come in handy.

Finally, you have to learn to be comfortable trying to hit a moving target. This field is constantly evolving and today's best practices are replaced tomorrow. The degree will give you a foundation of knowledge, but you will be constantly learning in order to stay up with current trends.

What is important to you when choosing a school or program?

I started with a basic set of criteria that included things like an accredited institution that was well-established and respected. After that, I focused on the program details. It was important that the program be offered fully online so it could be conveniently worked into my schedule. I wanted a curriculum that offered hands-on, practical experience.

A major selling point that the University of South Florida offered was having the

Florida Center for Cybersecurity right on campus. The center hosts a conference every year, as well as a series of sponsored events and guest speakers. These events create a unique opportunity to meet and speak with other members in the field.

What's the most fascinating thing you have learned during your studies?

We reviewed a lot of case studies about the recent data breaches at Target, Home Depot, JP Morgan Chase—and the list goes on. I think what I've found the most fascinating is that so many of these breaches were not the result of poorly designed tech. Often, they were human error or the result of bad decisions.

It's clear that organizations need to make just as much of an investment into training staff as they do into technology. A steel reinforced front door won't help if someone breaks in through a side window.

How can we encourage more students to pursue a career in cybersecurity?

The industry has certainly received a lot of media coverage in recent years, but I think there's still a lack of awareness regarding many of the cybersecurity opportunities. Security consists of many different areas including gathering forensic evidence for law enforcement, preventing cyber terrorism for the federal government and private sector opportunities, such as securing data centers and developing secure software. Sharing this information through events, hack-a-thons or any other means available may help encourage students to consider the security field.

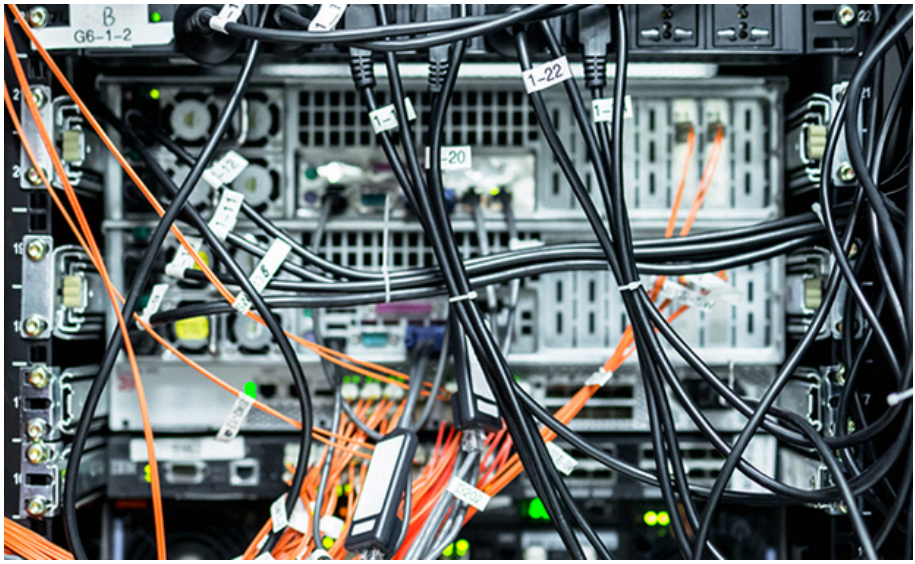
Businesses should also consider creating internships specifically dedicated to cybersecurity. The job market may be hot, but many of the entry-level security positions require more experience than most students would have immediately after graduating. Prospective students consider job prospects after earning a degree as part of their decision making process, and if they worry the degree may not be enough to get started, it presents an obstacle. If organizations want to fill some of these talent gaps, they should make internships available so that students can acquire additional skills and experience with real exposure to the type of work they will be doing.

In terms of your professional career, where do you hope to be in five years?

There is a lot of ongoing debate about privacy laws and the responsibility of

corporations to keep data safe. As more businesses try to balance convenience with security, new challenges will arise. I hope to help these companies with the strategic planning of their technology infrastructure and development efforts.

What Is the Next Phase of Cybercrime?



I recently got to sit down and discuss the future of cybercrime with Steph Aldridge, who may just be a contender for having the world's coolest job title: Cyber Assurance Bletchley Park; CyberCenturion and Diversity Lead at UK Cyber Security Challenge. Our conversation centered on the fact that we seem to be at a low point in the battle against cybercrime but that there is hope on the horizon.

Assessing loss

Looking at the big picture it's easy to be disheartened. In March 2014, Dell SecureWorks reported CryptoWall earned $34,000 in its first month of operation and by August 2014 had earned more than $1.1 million. In June 2015, the FBI's Internet Crime Complaint Center stated that 992 CryptoWall-related complaints were filed with resulting losses of more than $18 million.

Despite these losses, we need to keep our perspective. Until there is less money being made legitimately online than cybercrime is grabbing, the situation is significant but not catastrophic. Businesses will still go online and leverage an

online presence for their services. This might explain why the criminal element is moving towards ransomware attacks and away from mega breaches.

While I don't think mega breaches will stop anytime soon, they do create big headaches when it comes to monetizing the illicit haul of data. You need money mules and credit card processors, and it could take weeks to get your cash into hand. Don't discount the attentions of law enforcement either; a big breach can bring the heat down on even the best cybercrime gang.

> "A perhaps more alarming trend is that cybercrime is attracting more and more generalized criminals."

Held for ransom

As annoying as ransomware is – it's petty theft. It's lots of petty theft for sure but from a law enforcement perspective much of it goes under the radar. With "damage" around $300 to $1000 per instance, it's the cyber equivalent of "if you don't pay me $100 dollars I'll break your car window."

A perhaps more alarming trend is that cybercrime is attracting more and more generalized criminals. This is underscored by a recent University of Cambridge study, which showed that 60 percent of cyber-criminals had a record unrelated to cybercrime. This isn't totally surprising given that the consequences are minimal and entry is easy—utilizing Crime as a Service (CaaS) providers bringing everything together in one neat package.

Based on all of this data, staffing levels in electronic and cybercrimes have to be adjusted. The people that were doing breaking and entering, or mugging, are not suddenly going to become the next Lex Luthers of cybercrime, so we have plenty of leeway to stop them. But we do need to stop them.

Sheep and wolves

This brings me to my final point. If we look at the cybercriminals as wolves and the victim businesses as sheep, you need to ask the question: What happens when the wolves outnumber the sheep? Would businesses go online anymore? Very probably not.

Keep in mind that the folks supplying CaaS – the real Lex Luthers of cybercrime – are not dumb. They know they have the capability to destroy business online and

they have had a great run of looting and pillaging. Yet, like the pirates of the 17th century had their comeuppance, I think ransomware suppliers may fade into the cyber history books over the coming years; because ultimately if they destroy the very thing they feed off they no longer have any reason to exist.

FBI Director James Comey summed things up nicely when he described the internet as “the most dangerous parking lot imaginable,” and warned people to be just as aware of scams, compromised websites, malware and other threats as they would be of a physical theft.

So where will the cybercriminals go next? My money is on the Internet of Things. How they will turn it into a criminal payday is yet to be seen, but whatever happens, we the defenders will do what we do best: defend our networks.

About Us

Who we are

Today's challenges cannot be solved with one-size-fits-all solutions. From improving workplace wellness to weighing the competitive advantages of cloud computing, we want to help you pioneer the future.

What we do

We are storytellers with a purpose. Mediaplanet specializes in content creation and distribution through various multimedia platforms. We provide our readers with insightful and educational editorial in the fields of their interest, designed to motivate them to take action. We continue to explore and expand our network of partners and clients through the shared interest of providing readers with the best experience possible.

Visit our website to learn more.

To follow us more closely, check out our social accounts: