softchoice

ISSUE #3 WINTER 2017

THE ULTIMATE SECURITY GUIDE

THE TROUBLE WITH RANSOMWARE

UNDER PRESSURE: CLOUD SECURITY

YOUR HEALTHCARE ORG'S BIGGEST THREAT

BRIDGING THE SECURITY TALENT GAP

THE NEW THREAT FRONTIER OF IoT

DECIPHERING THE CRYPTO WARS

THE UNDERGROUND MALWARE ECONOMY

TOP SECURITY EXPERTS REFLECT ON 2016'S BIGGEST THREATS, AND WHAT HAPPENS NEXT

ULTIMATE SECURITY GUIDE

PLATINUM SPONSOR

IBM

GOLD SPONSORS

intel Security

KASPERSKY lab

SONICWALL

SOPHOS

TREND MICRO

SILVER SPONSORS

Barracuda

BlackBerry

eset ENJOY SAFER TECHNOLOGY

FORTINET FAST. SECURE. GLOBAL.

Malwarebytes


Cognitive security is here.
When everything is connected, everything is vulnerable. IBM uses cognitive technology to help protect the critical assets of your business. It senses and helps detect millions of hidden threats from millions of sources, and continuously learns how to defeat them. When your business thinks, you can outthink attacks.
outthink
threats
IBM and its logo and ibm.com are trademarks of International Business Machines Corp, registered in many jurisdictions worldwide. See current list at ibm.com/trademark. Other product and service names might be trademarks of IBM or other companies. ©International Business Machines Corp. 2015. P31409
Learn more about cognitive security.

WELCOME TO THE SOFTCHOICE ULTIMATE SECURITY GUIDE

Dear reader,

As we all understand, security has not gotten any easier over the last year as major media outlets report on data leaks, ransomware and other attacks that paralyzed businesses around the world. I have spoken with many clients personally, and came to the realization that there is no simple or single solution that guarantees total security for your business.

When you really think about it, how can there be?

It is no longer enough to throw money at perimeter-fortifying technology in the hopes that it will stop hackers in their tracks. As a matter of fact, adding more technology is only worsening the problem.

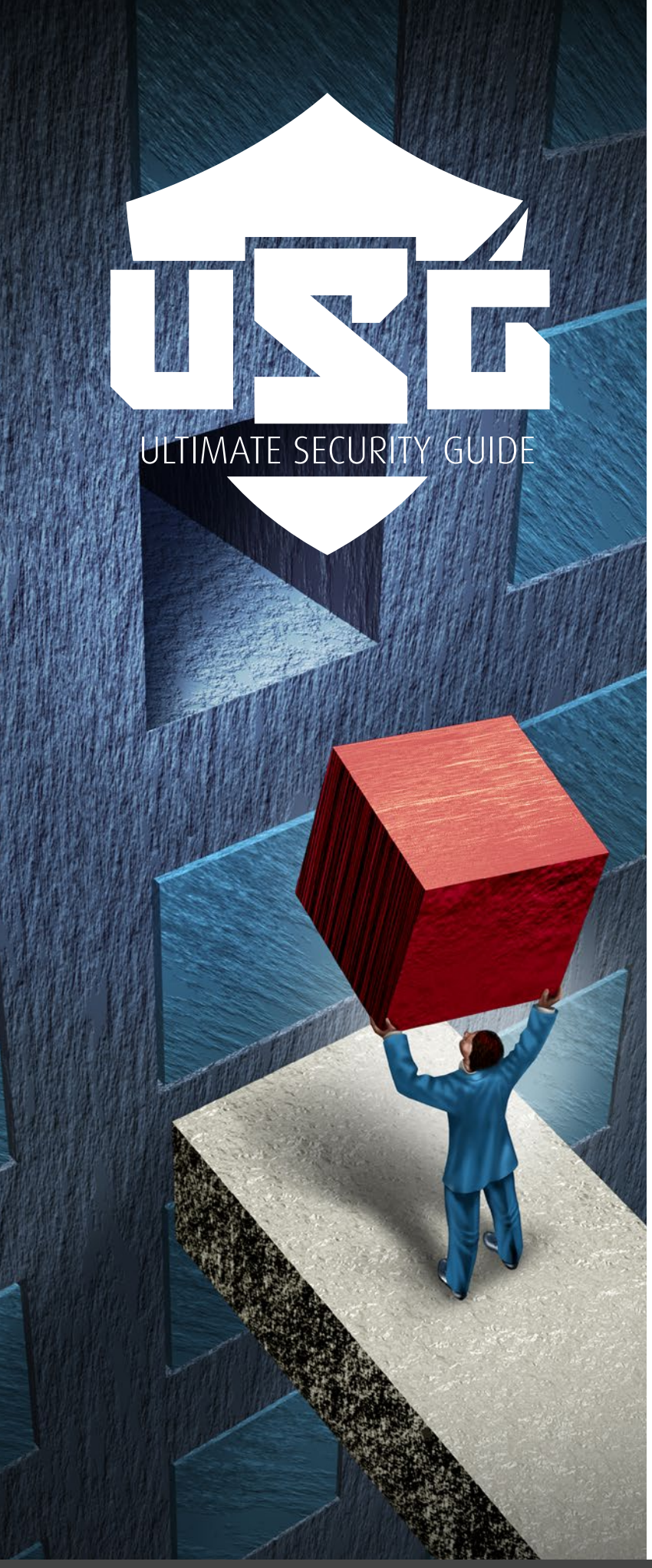
According to a recent PWC report, companies have increased their security spend by 24%, yet security incidents have also increased by 38%. This is not surprising given the challenges you're faced with – whether it be lack of resources, training, compliance, prioritizing new solutions, or dealing with the aftermath of an attack.

IT leaders across North America echoed these challenges with us this summer, when Softchoice hosted its first Security Innovation Executive Forum. Their concerns rang loud and clear: Securing the immediate IT environment is simply not enough. I encourage each client I speak with to truly rethink and modernize how they approach the concept of security, and that conversation has inspired us to develop our first Security Point of View . The Security Point of View serves as a framework that builds a new path to security for our clients to follow.

To help you understand what leaders in the industry are seeing, I am happy to introduce our current edition of the Ultimate Security Guide. In this edition, we interviewed top leaders in IT security to gain a more in-depth understanding of what we are up against. Their insight will challenge you to think about security differently. At least, I hope it will.

I would like to thank all our partners for being part of this journey with us and to you for taking the time again to read this guide.

George Myrtos
Category Lead, Business Development
Softchoice Enterprise Software & Security



WINTER 2017

ISSUE 3

COMPLETE LIST. WHAT'S IN THIS ISSUE

- ULTIMATE SECURITY GUIDE SPONSORS
  PAGE 02
- WELCOME LETTER
  PAGE 04
- THE TROUBLE WITH RANSOMWARE
  PAGE 08
- THE VAST UNDERGROUND MALWARE ECONOMY
  PAGE 10
- DECIPHERING THE CRYPTO-WARS
  PAGE 12
- NEW TECH WILL BRIDGE THE SECURITY TALENT GAP
  PAGE 14
- WHAT'S THE GREATEST SECURITY THREAT TO YOUR HEALTHCARE ORGANIZATION?
  PAGE 16
- UNDER PRESSURE: THE CLOUD SECURITY BURDEN
  PAGE 18
- LETTER FROM A HACKER: THE NEW FRONTIER OF THE IoT
  PAGE 20

MEET OUR DEDICATED SECURITY TEAM

ANDREA KNOBLAUCH
PreSales Technical Architect

ANDREW CAMPBELL
PreSales Technical Architect

ALEXANDRA LEE
PreSales Technical Architect

GEORGE MYRTOS
Category Lead, Enterprise Software and Security

JEFF KROTH
Security PreSales Architect

JEREMY BANDLEY
PreSales Technical Architect

MIKE COIT
PreSales Security Architect

MIKE STINES
PreSales Security Architect

TREVOR MULVIHILL
PreSales Technical Architect

CONTRIBUTORS

ANGELI GHELANI
Marketing Coordinator

AYUMI BUCKLE
Marketing Database Lead

CHELSEY BYNG
Marketing Operations Lead

EMILY DAVIDSON
Digital Marketing Lead

KARLY PIERCE
Marketing Manager

MARTIN PIETRZAK
Digital Marketing Supervisor

MICK WARNER
Marketing Enablement Supervisor

PATRYK BOGNAT
Graphic Design

ADVERTISING INQUIRIES

GEORGE MYRTOS
Category Lead
Enterprise Software and Security
George.Myrtos@softchoice.com

ULTIMATE SECURITY GUIDE

WINTER 2017 - ISSUE 3

PLATINUM SPONSOR
IBM

GOLD SPONSORS
Intel Security
Kaspersky
SonicWall
Sophos
Trend Micro

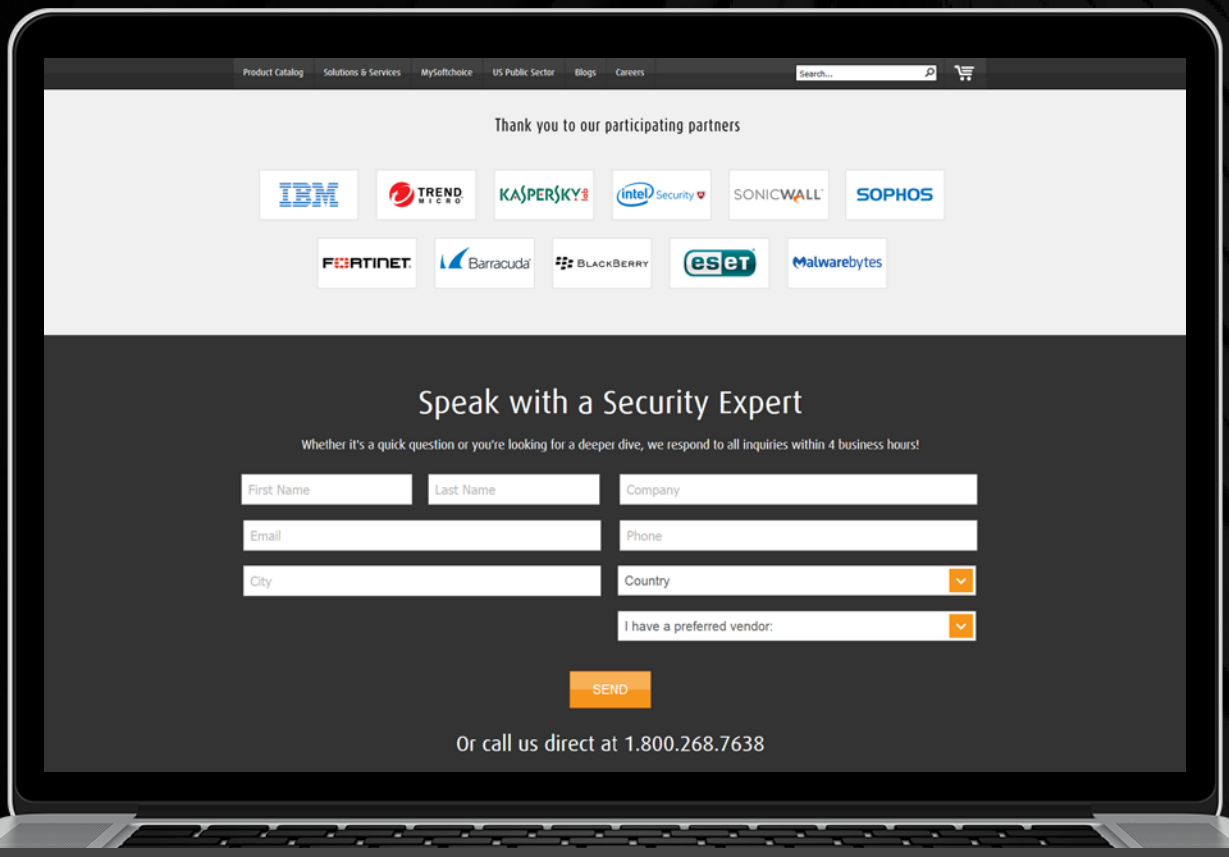
SILVER SPONSORS
Barracuda
Blackberry
ESET
Fortinet
Malwarebytes

THE ULTIMATE HUB FOR SECURITY

Visit Our Microsite To Access:

Free Assessment Tool
How-To Content From Our Partners
The Latest Security News And Updates

>> Access the Microsite Now <<



softchoice

THE TROUBLE WITH RANSOMWARE

Fabian Ubogi, Sales Engineer at Intel Security, has a problem: nobody takes the threat of ransomware seriously enough.

"It's going to happen to them. If it hasn't already, it's just a matter of time," says Ubogi. "A lot of people thought 'It's not going to happen to me,' and they're now my customers. Because they got hit."

What makes ransomware different from any other type of malware or virus? And why has it escalated to the point where Ubogi calls it a matter of "life and death" without a hint of exaggeration?

AN UNREASONABLE DEMAND

Ransomware evolved from the idea of a hacker using malware to encrypt data on a user or corporation's device and refusing to decrypt it until they receive payment. This threat has existed since the 1990s, but until recently, it was considered an impractical ploy for the bad guys.

Why? Because attempts by hackers to secure blackmail funds through money orders or cash sent to P.O. boxes provided enough of a paper trail for police to track down the perpetrators. Ransomware attackers simply lacked a way for the victim to send payment without exposing the attackers to risk.

So ransomware never really took off until the advent of a more recent digital innovation: untraceable cryptocurrency.

MONEY MATTERS

In 2009, the inventors of Bitcoin introduced the world to a universal and completely decentralized form of cryptocurrency. The hacker community took notice.

Since Bitcoin transactions are not tethered to a physical location, they are extremely hard to track. The bad guys finally had the answer they were looking for. With an easy, risk-free way to collect payment, according to Intel Security, ransomware attacks spiked from 300,000 in the fourth quarter of 2014 to almost 800,000 in the first quarter of 2015.

THE USUAL TARGETS

The goal of ransomware is for the bad guys to sell a person's data back to them after hacking into their system and blocking access to their files. So the target of these attacks is different than with other types of malware like keyloggers, spyware and botnets that simply exploit personal information.

Not to say that average users and employees aren't affected by ransomware -- they are, and frequently -- but the most lucrative and terrifying targets are often governmental agencies.

"The biggest problem I see with the government sector is outdated security technology and the slow pace of upgrading. They simply don't have the budget or the resources to implement the technologies they need to protect themselves."

Ransomware attacks on government are widespread. In fact, the U.S. Congress suffered so many attacks this past year that they consulted Yahoo on how to protect their Yahoo Mail accounts - and then Yahoo was hacked. According to Ubogi, the mix of outdated technology and underfunded security measures in Government IT makes them an enduring target for hackers.

"[Hackers] are aware of the situation, and they're taking advantage of it. Protecting healthcare patients' records and data is very important -- it could be the matter of saving a life or not," he says.

THE RANSOMWARE ATTACK THAT CAUGHT HIS ATTENTION

In February 2016, the Hollywood Presbyterian Medical Center in Los Angeles was the target of a ransomware attack that denied employees access to the hospital's computer network and medical records.

"The part that's really scary is that the hospital had to shut down a lot of machines... the outage lasted for a week," says Ubogi. "Patients had to be diverted to other hospitals, recordkeeping was maintained using pen and paper. And this infection came from a malicious link."

After consulting and weighing options, the hospital decided to pay the ransom of 40 Bitcoins (around $17,000 USD) to retrieve access to their files as quickly as possible.

Ubogi says that the issue of paying out a ransomware attack is a contextual decision, but that he always advises against it for a simple reason: "If [hackers are requesting] a thousand dollars and the data is worth millions, there's no issue. But hackers will see that if you paid once, you'll pay again. It makes you a target."

HOW TO AVOID YOUR OWN HOSTAGE SITUATION

Ransomware isn't going anywhere. Ubogi admits that he tracks Google Alerts for new strains of the malware with advances being made on a daily basis - especially when it comes to exploit kits. In the battle against ransomware, Intel Security is working with law enforcement agencies on operations against a number of

ransomware families. But they won't reveal the details. They are also a founding member of the Cyber Threat Alliance: a group of leading cybersecurity solutions providers who have come together to share threat intelligence on advanced attacks and the tactics of the actors behind them.

When it comes to protecting your data from an attack, he recommends a two-pronged protection plan of vigilance and education.

"Be suspicious," says Ubogi. "The majority of ransomware vectors come from email and websites. Every email, every link you click, you need to be suspicious. You need to start from there; it's a mind state we need to change." This means building a "human firewall" to stop users from letting ransomware onto their endpoints. People are the weakest link.

Next, consider spam and web gateway filtering technologies to keep ransomware from reaching endpoint devices in the first place. Then, apply all current operating system and application patches. Having the latest operating system, application versions and patches reduces the attack surface to a minimum. Lastly, use an application control method that will only allow whitelisted items to execute: blocking unauthorized executables on servers, desktops and fixed-function devices. These tips, when used together, can dramatically reduce the attack surface for most ransomware.

Going back to his first point, Ubogi says the most important step of all is still widespread training across every organization. "It comes down to more training -- as much as we don't like it. We need more training to make us more aware of what threats are out there."

WHAT TO DO WHEN YOU DETECT MALWARE

If you suspect your device has picked up malware or is being targeted for a ransomware attack, Ubogi doesn't mince words about what you need to do next: "Quarantine and format."

Do not enable macros in documents received via email until you know they're safe. Then, write access control rules against targeted file extensions that deny writes by unapproved application processes. Doing so will complement your host intrusion prevention system with a similar strategy. Once a process is flagged as suspicious, send it to a security sandboxing appliance for further study.

Because, as he said before, it's no longer a question of if you'll be a victim of a ransomware attack, but when. The data supports his statement.

WE NEED TO BE PROACTIVE, AND WE NEED TO DO IT NOW

Ubogi's ideal approach of increased security infrastructure and widespread education is possible when IT teams and corporations take the threat as seriously as he does.

He says that the era of the Internet of Things only throws more variables into the equation, because every new network-capable device in the workplace adds another opportunity for inter-perimeter infection. Everyone involved, from employees to CEOs to IT managers, needs to step up their game and be ready to repel the inevitable ransomware attack.

Because it's coming.

THE VAST UNDERGROUND MALWARE ECONOMY

Modular development, regular feature upgrades, online reviews and first class technical support: if you think these are the bread and butter of software manufacturers alone, it's time to think again.

According to Christopher Budd, Global Threat Communications Manager at Trend Micro, "These are now common practices among today's thriving underground malware economy."

Long gone are the days of teenagers crafting the latest threats in dark basements and blasting them into the wild. Today, companies face a vast underground malware and ransomware economy comprised of organizations and networks as complex and capable as the mainstream software vendors they target every day.

In our latest interview, Budd reveals the shocking scope of today's underground threat economy and some practical ways organizations can protect themselves from this growing threat.

MALWARE HAS BECOME A FULLY MATURE AND ROBUST SHADOW SOFTWARE ECONOMY

"It's a sophisticated ecosystem consisting of sales, customer support, testing and advertising," Budd says. Much of the malware available on the underground market today has professional aspects -- such as modular development and regular upgrades with new features-- that draw from the best practices of legitimate software development companies and services.

"We've seen underground sales forums with banner ads boasting malware that have been tested and guaranteed to be undetectable by the latest top enterprise security solutions. Malware often comes with technical support, including online chat, that's often better than the support you get with legitimate software."

If you're familiar with eBay and Amazon.com, you know the value of positive online customer feedback. Budd describes the malware economy as dependent on positive word of mouth -- often so valuable for advertising purposes that organizations willingly exchange millions of stolen records for nothing but positive feedback on peer-reviewed malware market boards.

And it works. As Budd reveals: "Hackers save tremendous amounts of time and resources by purchasing malware from underground markets. When they do, they receive capabilities much more sophisticated than what they could have ever built alone."

RANSOMWARE CREATORS UNDERSTAND THE STRESS OF DATA LOSS

Ransomware, in particular, is one of the most powerful, sophisticated and pernicious forms of malware ever devised-- on both the technical and social engineering sides.

"Today's ransomware often incorporates deadlines that give the victim, say, three days to pay a ransom or have the encryption key that unlocks their stolen data destroyed," says Budd. These deadlines create a sense of urgency in the victim that often leads to a hasty decision to pay the hackers and get it over with.

Since many ransomware threats require payment through Bitcoin, hackers even offer chat support to help the victim set up a payment method using this untraceable cryptocurrency.

HOW DO ORGANIZATIONS CRAFT AN EFFECTIVE DEFENSE? ADAPT

"Eighty percent of malware today infects five or fewer systems. Much of what we see is designed to alter as it works so that one person may get hit with a different version of the same malware multiple times," Budd says. Which means that traditional static defenses can no longer meet such a threat. He continues, "Instead, it's important to focus on strategies and solutions that employ heuristics [non-perfect yet agile approaches] and other intelligent defenses that adapt continually to changing attacks."

Budd describes a multilayered defense with adaptability, intelligence and defensive strategies like effective backup, that lie outside the realm of security-focused solutions. With a robust backup strategy that can get the CEO up-and-running with zero effective data loss in an hour, there's nothing to worry about from ransomware.

"It's important to have a full awareness of all the things touching your data. Defense today is all about protecting the data, not the perimeter, devices, and networks."

Usability and comprehension are also key requirements in any security solution. A solution that boasts comprehensive protection but is impossible to configure and use is flawed. "If you can't set up an advanced solution properly, you're just as much at risk as you are with a less capable solution," Budd says.

Finally, testing and drills are the best way to know how well your defenses are working. For example, say the CEO's laptop was just stolen, you need to test how effectively you can replace it with everything intact.

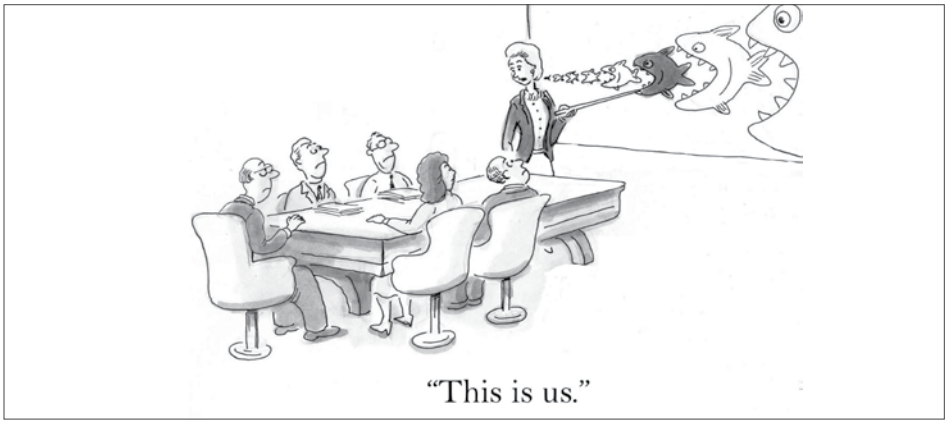
TEST IT ON A REGULAR BASIS

What to do if your information gets hijacked

If you're attacked, Budd advises you to go back to training. "Assess the situation, determine exactly what happened, what the malware is doing and the technical specifics involved. Disconnect affected systems from the network to prevent it from spreading. If the attack employed ransomware, look for a backup and recovery solution," he says.

He also advises that if you can't take systems offline without disrupting the business, to make sure that you find and test solutions and strategies that can assess, isolate and address the issue and the specific systems involved while the business continues to operate normally. "Most organizations should be at the point where they can handle an incident or compromise to a certain level without a total shutdown."

Every attack is different, but Budd's universal advice is, don't panic.



DECIPHERING THE CRYPTO WARS

Many governments seek to reduce access to strong encryption technology for national security reasons. Enter "crypto wars"-- battles over government attempts to obtain access to encryption keys or to prevent the public or foreign powers from accessing strong encryption. The paradox is that the whole idea of data encryption loses its purpose if backdoors are created to circumvent it.

Kaspersky Labs' Security Evangelist, David Balcar, believes it's crucial for businesses to keep their encryption as hard and unbreakable as possible.

"It's a matter of consumer trust," says Balcar, who is responsible for supporting Kaspersky's enterprise Anti-Targeted Attack Platform and Security Intelligence Services. Companies that don't take threats to encryption technology seriously risk losing customers along with their hard-earned confidence.

"Imagine a bank that has the encryption between itself and customers compromised and does nothing to correct it. Who is going to want to conduct online banking with them?" Balcar asks. "If the bank's mortgage brokers are in the field and their devices cannot be trusted to safeguard customer data, then the bank can't conduct business. It's a huge issue."

BLURRED LINES PUBLIC'S SECURITY VS. YOUR PRIVACY

Security is a continuous battle between the "good guys" and the "bad guys". But the line blurs with the addition of government agencies seeking to access encrypted data for national security purposes or to aid law enforcement.

Brought under the public spotlight during the 2013 Snowden leak, the "crypto wars" rage on. For example, in early 2016, the FBI obtained court orders to have Apple create software to unlock an iPhone recovered from one of the terrorist shooters in an attack in San Bernardino, California. The company refused.

"On one hand, you have the governments saying, 'We need the ability to see all the data.' But people have an inherent right to privacy," he says. "How do you balance the public's right to privacy with the police force's ability to keep us safe? It's a slippery slope."

Balcar says there are always methods by which law enforcement can run investigations without being given backdoor access to encrypted data. "In the case of San Bernardino, law enforcement eventually paid $1 million to have someone crack the phone. Now Apple is suing them to find out how, so they can prevent it from happening again in the future." When a backdoor exists, it is only a matter of time before cyber criminals can find and exploit it. And let's not forget the Clipper chip debacle from a few years ago.

UPPING ENCRYPTION EFFORTS ENCRYPTION BY DEFAULT

Balcar says companies like Apple and Google are recognizing consumers' increased desire for security, and continue to ramp up the encryption technology incorporated in their products. Both companies have started to encrypt their mobile devices by default, rather than leaving them for customers to configure.

"And they've made the encryption so strong that even governments can't decrypt it," Balcar says. "The governments of the world can't expect to have a backdoor into someone's encrypted data and communications, because all backdoors eventually get discovered and used for bad things."

"It's a question of who's watching the watchers," adds Balcar. "I don't know of a single company that would want the government to have access to all their private data."

- **PASSWORD REUSE CONTINUES TO BE A THREAT**

According to Balcar, despite the hype around quantum computing's ability to hack state of the art encryption, one of the biggest risks companies face today is the common practice of reusing passwords across different systems.

"If one password is hacked, it doesn't take a quantum computer to hack the others if they are the same," he notes. "You've made the hacker's job super-easy."

Balcar sees quantum computing as a direct threat to current encryption algorithms, but it's unlikely that cybercriminals will need to take advantage right now, since ongoing password dumps on the Internet make their work even easier. Some of these dumps result from improper use of encryption or the lack of it, so how can you be sure your password is secure on a 3rd party site?

"Only time will tell," he adds, "Quantum computing is a phenomenal next step in encryption and decryption technology. But it isn't really in the hands of cybercriminals. Only research universities and a few companies around the world are utilizing this. Quantum computing is still in its infancy." A research paper published in 2012 outlines that Quantum Cryptography can be attacked in a "man-in-the-middle" attack.

COMPANIES ARE ONLY AS VIGILANT AS THEIR SECURITY STRATEGY

"Look closely at the options available and test them for your environment, because there is no silver bullet," Balcar continues. He provides IT and security managers with a few key tips:

- Check your encryption methods and make sure they are working. If you are using DES (Data Encryption Standard), which is known to be breakable, Balcar suggests upgrading to AES (Advanced Encryption Standard) or higher forms of encryption.
- Stay informed about what's happening on the security landscape -- not just what is affecting your company, but also your industry as a whole.
- Look at security as "layers of an onion". Don't just consider the encryption of your data at rest, but also the encryption needs for data in transmission.
- Clarify what needs to be secured and at what level. "You might not need to encrypt the monthly newsletter," Balcar says, "but the company's intellectual property -- a chemical formula or the Colonel's secret recipe-- is something that needs to be protected. Start with what's most important."

In addition to maintaining strong encryption algorithms and enforcing good password policies, Balcar suggests a company's security strategy must be holistic.

ENCRYPTION IS, OF COURSE, JUST ONE PART OF THE EQUATION.

NEW TECH WILL BRIDGE THE SECURITY TALENT GAP

A SHORTAGE OF IT SECURITY STAFF, A MOUNTAIN OF UNSTRUCTURED DATA AND A GROWING NUMBER OF END-USER DEVICES CREATE A PERFECT RECIPE FOR A GRAND SECURITY THREAT

According to IDC and EMC, the world's data is projected to explode to 40 zettabytes (a.k.a. 40 billion terabytes) by 2020. That represents an exponential growth of 50 times in just 10 years!

What's worse, 70%-80% of all data in organizations is unstructured data-- data not organized in ways that today's machines can read easily -- think natural language like emails or presentations rather than structured data like tables in a database.

The never-ending open faucet of data pours in from threat intelligence, network, advance fraud, identity access management, data applications, mobile and endpoint tools and research documents.

The problem: security teams have to stay on top of this data to prevent new security breaches.

SECURITY TOOLS ARE NOT THE ANSWER

"On average, you have 85 security tools from 45 vendors that you're trying to use," says Willie Wong, Canadian Marketing Leader for Security at IBM. To stay protected, we need to keep on top of constant change and an onslaught of information.

Organizations must wake up to the fact that technology is only one aspect of the solution to security issues. Wong continues, "A lot of organizations focus only on the technology." More technology doesn't mean lesser problems. In reality, more tools deepen the knowledge gap of your IT pros. And, that gap is widening.

By 2020, the IT industry will have 1.5 million open security positions and not enough graduates to fill essential jobs. Organizations are fighting for the best candidates, but the reality is that amidst overwhelming data growth, they won't be able to recruit fast enough.

EVEN THE LARGEST ORGANIZATIONS CAN'T AFFORD TO HIRE 1000 SECURITY PEOPLE

According to IBM, most security teams only have the power to decipher 8% of incoming unstructured data to protect their environments. Trying to keep up with this constantly growing data forces a more perimeter-focused reactive approach. But what if there was a fine-tuned Artificial Intelligence (AI) system that could analyze all that data for you? Expert systems like this not only seek out and collect the data, they are also designed to develop human-like capabilities for learning. This kind of system could give even the smallest teams the ability to process huge amounts of information about what's happening both inside and outside their perimeters.

ARTIFICIAL INTELLIGENCE HOLDS THE CAPABILITY TO TURN A TEAM OF FIVE INTO 5000

IBM is doing just that with the latest iteration of their Watson platform that leverages cognitive technology and according to IBM, "can think like a human".

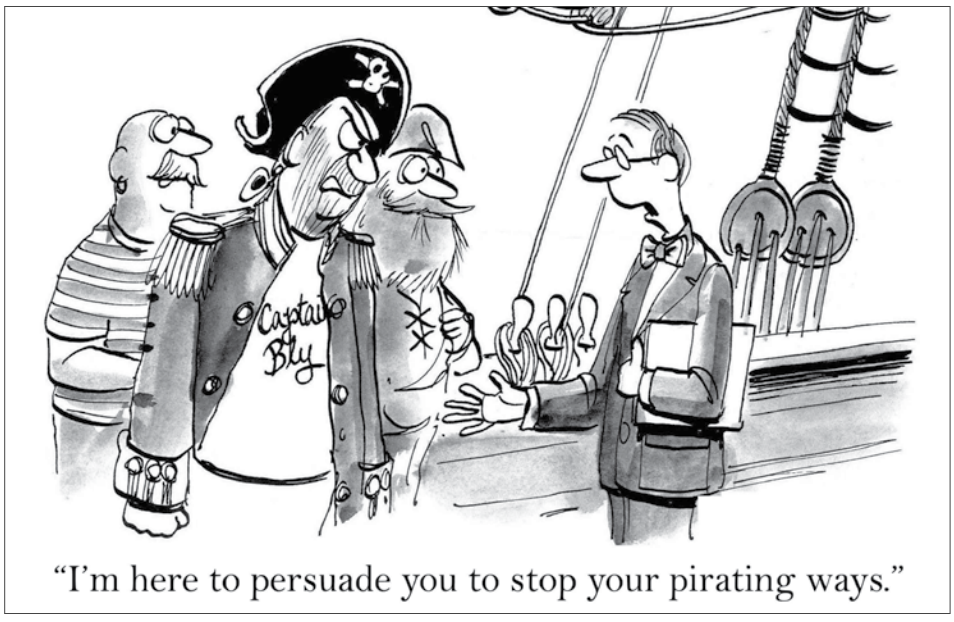
"We're going to integrate Watson's AI with QRadar [a security information and event management solution] and the IBM security suite, so it's all-in-one," reveals Wong. Once Watson's AI has algorithms from all of the security tools, it will analyze unstructured data, crunch the numbers, pull out the evidence and assess and rank the biggest risks. This includes capabilities to identify internal user threats quickly, based on unusual user behavior patterns.

This is not a replacement for a team of security experts, it's a turbo boost for their information analysis power. Expert systems like Watson provide information to human analysts, who review the information and take action. This prevents Watson's AI from making decisions on behalf of the analyst, like shutting down business critical systems without asking. It also frees up your experts to do the important work and leaves the more tedious work to the AI.

EVEN AI SOLUTIONS AS WELL KNOWN AS WATSON STILL HAVE A LOT TO LEARN

Watson isn't quite ready yet, "We had to send Watson back to school," Wong replies. "And, there are eleven universities involved globally to teach Watson the language of security. Coming out of that, we will probably start doing prototyping. We have ten organizations globally already signed up for beta testing. We can't talk about them, but two of them are financial institutions. They want this quickly."

In the meantime, Wong advises immediately educating all employees to accurately identify what they should and absolutely should not access while on your network. Until systems like Watson are ready, a plan that makes employees aware of these risks and reduces internal risks is essential for tightening security on the inside.



"I'm here to persuade you to stop your pirating ways."

WHAT'S THE GREATEST SECURITY THREAT TO YOUR HEALTHCARE ORGANIZATION?

Look in the mirror. You may have a robust, compliant security infrastructure in place, but all it takes is one employee to click on a phishing email to compromise your network and your data.

Healthcare organizations struggle to stay secure and compliant with HIPAA and PCI in an environment of constant, changing threats. We interviewed Brook Chelmo, Senior Marketing Manager at SonicWALL, about the steep challenges these organizations face. His overarching message? Those that rely on check-box compliance for security do so at their peril.

Here's what Mr. Chelmo said about how regulated organizations can stay safe.

CHECKMARK COMPLIANCE DOES NOT MAKE A ROBUST SECURITY SOLUTION

Vendors like to beat customers over the head with compliance because it leads to more sales. But if an organization focuses too heavily on compliance, it can achieve "checkmark security" while leaving itself wide open to attack. Let's unpack this a little.

Are you encrypting data in transit and at rest? Are you protecting your data in a way that makes sense to your environment? Have you considered the physician who brings his or her work laptop or mobile device home?

How is your content filtering solution configured? What is it capable of? Are employees checking Facebook on breaks? Are they googling Black Friday deals and ending up on sites that inject malware or steal payment data? Many of these concerns are not likely to be covered by compliance checkboxes.

AT THE END OF THE DAY, SECURITY IS ABOUT EMPLOYEE TRAINING

I don't think there are compliance checkboxes for running employee phishing tests every three months. Those are the best practices that really help you stay secure.

The truth is that most IT managers look at compliance as a sword of Damocles, not a comfort.

If you're responsible for personal data, you risk steep compliance fines. Personally, I feel that a hospital should not be fined unless it's clear that its intention was not to comply. Instead, the should be allowed to invest that money back into the organization's security.

USE A NETWORK SANDBOX SOLUTION TO DETONATE THREATS

Hackers create new malware variances every day. In the past year, we've detected 64 million pieces of unique malware and blocked 2.2 trillion IPS attacks. That's why we developed a network sandbox solution called Capture ATP. If the firewall detects suspicious code, Capture ATP takes it to an isolated and protected environment in the cloud and runs the code to see exactly what it does.

Capture ATP uses a multi-engine strategy that detects malware-related actions at the application, operating system and hardware levels. Since the launch of the service on August 1, 2016, we have uncovered over 1400 brand-new variants of malware. Our customers have an extra layer of protection that offers good performance, reporting and automation so they don't have to monitor their traffic all of the time.

IN MOST ORGANIZATIONS, PEOPLE ARE THE WEAKEST SECURITY LINK.

Email addresses, even the CIO's, are always available and easy to exploit. For example, a hacker could spoof a marketing director's email with a message that says, "I have an interview coming up and attached is a list of questions." All it takes is one person to open the attachment and now you have ransomware or a Trojan behind the firewall. That's why employee training and phishing tests are so important.

Also important -- get a good next-generation firewall, ensure you have ways to detect attacks when they happen and ways to stop the exfiltration of data and make sure your solutions can protect from malware hidden in encrypted traffic.

You need a good mobile endpoint protection strategy that stops malware from infecting mobile devices when they're outside the network. You also need multi-factor authentication so hackers can't access your network after they start hacking connections through public Wi-Fi.

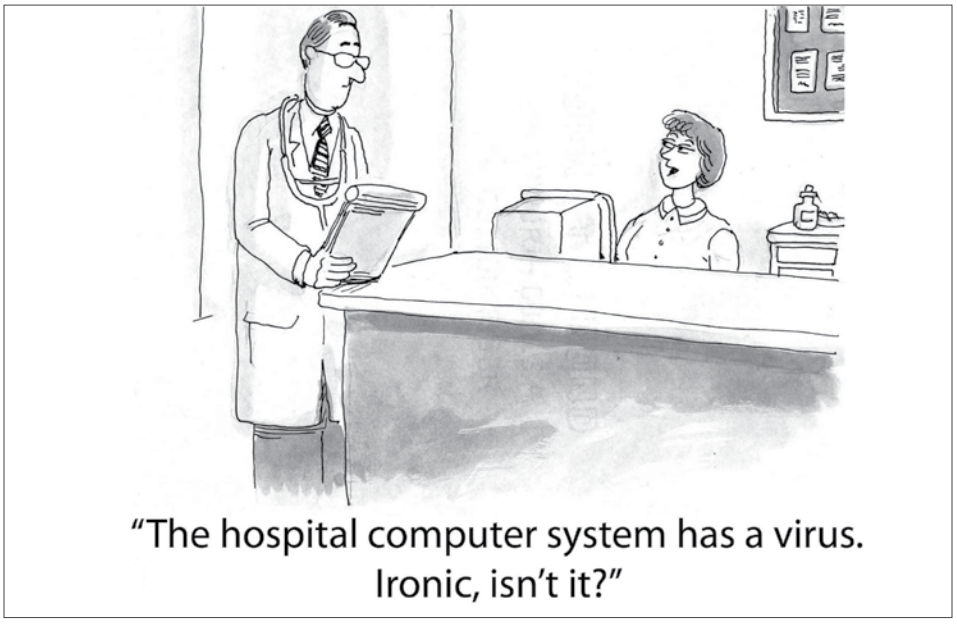
WHEN IT COMES TO DETERMINING YOUR SECURITY BUDGET, CONSIDER THE BLACK MARKET VALUE OF YOUR DATA

If I were to hack your hospital network, what would the data be worth on the market? Is your security budget in line with this number? Even so, security is always a balance between fortification, access and inspection. You can't put in so many security solutions and policies that it's difficult for employees to get to the network or customers to the website.

TO ASSESS RISK, GO HACK YOURSELF

Two words: penetration testing. Penetration testers help you find vulnerabilities and figure out how to protect yourself. Hire an outside organization to attempt to hack into your network and see how vulnerable you are. If your organization is spending $3 million securing medical records, spend $100,000 to make sure you're secure in all areas, not just the one or two that are most obvious.

Capture ATP data shows us that the average company gets hit by eight-to-ten new forms of malware or ransomware every year. All it takes is one attack to bring your organization to its knees.



UNDER PRESSURE: THE CLOUD SECURITY BURDEN

Most employees are under heavy time pressure. Most have too much to do and too little time to accomplish it. Placing additional security, data protection and computer-related duties on their shoulders only magnifies workday stress – and that leads to mistakes.

"People under stress will make mistakes, and that can leave the back door wide open to cyber criminals," says Marty Ward, Vice President of Product Marketing for End User Security and Cloud Solutions at Sophos. "Employees shouldn't have to care about whether their emails are encrypted or their data is secure."

THE WEAKEST LINK -- PEOPLE

The Verizon 2016 Data Breach Investigations Report (DBIR) backs up Ward's sentiments. It finds humans to be the weakest link in the vast majority of data breach incidents. Whether through phishing, improper disposal of information, misconfiguration of systems or lost devices, human error is at the root of most incursions.

The bad guys know this and they grow more sophisticated with each passing day. The study discovered that cyber criminals now lure more victims by crafting customized spam using regional vernacular, brands and payment methods. Ransomware cleverly disguised as authentic email notifications, complete with counterfeit logos, is even more believable and therefore more financially rewarding to the criminal. These scam emails impersonate local postal companies, tax and law enforcement agencies and utility firms, often including phony shipping notices, refunds, speeding tickets and electricity bills.

PASSING THE SECURITY BUCK TO THE CLOUD

The situation is worsened by the fact that many attempt to pass the security buck to the cloud. With cloud-based services being so pervasive in the enterprise, a dangerous misconception has emerged.

"Employees and even IT staff often assume incorrectly that their cloud provider has taken care of all their security needs," says Ward. "Many of these providers offer excellent security within their own infrastructure. But that doesn't mean user data is fully protected."

He uses the analogy of someone keeping money in a safe inside a house protected by a state-of-the-art home security system. Once that person walks outside the front door, the money in his or her pocket is no longer protected.

It's the same with cloud security. Data may be encrypted, firewalled and malware-free when it is inside the service provider's infrastructure. But when data is being transmitted to and from the cloud, it is at risk. Hackers know this and prey upon it.

AUTOMATED SECURITY: TAKING HUMAN RISK OUT OF THE EQUATION

Some companies leave it up to employees to encrypt sensitive emails or set security policies for their own data. All it takes is one slip and the entire network can be compromised.

"What it requires is an integrated approach to security with automated policies set at the

company level," says Ward. "It is possible to encrypt all data automatically whether it is at rest or in transit. You also need to set policy on what users can and can't do and where they can and can't go."

THE FOUR KEY AREAS FOR IT TO ADDRESS

Ward identifies four key areas that IT security must address: data, devices, network and applications. Comprehensive enterprise security must be synchronized across each of these four zones.

User data must be encrypted at all times without the user even having to be aware of it. The security perimeter must extend to every server, laptop, tablet or phone – and to every nook and cranny of the network.

Applications, too, must come in for special protection. According to the Verizon DBIR, web and cloud application attacks were responsible for the bulk of data disclosure incidents.

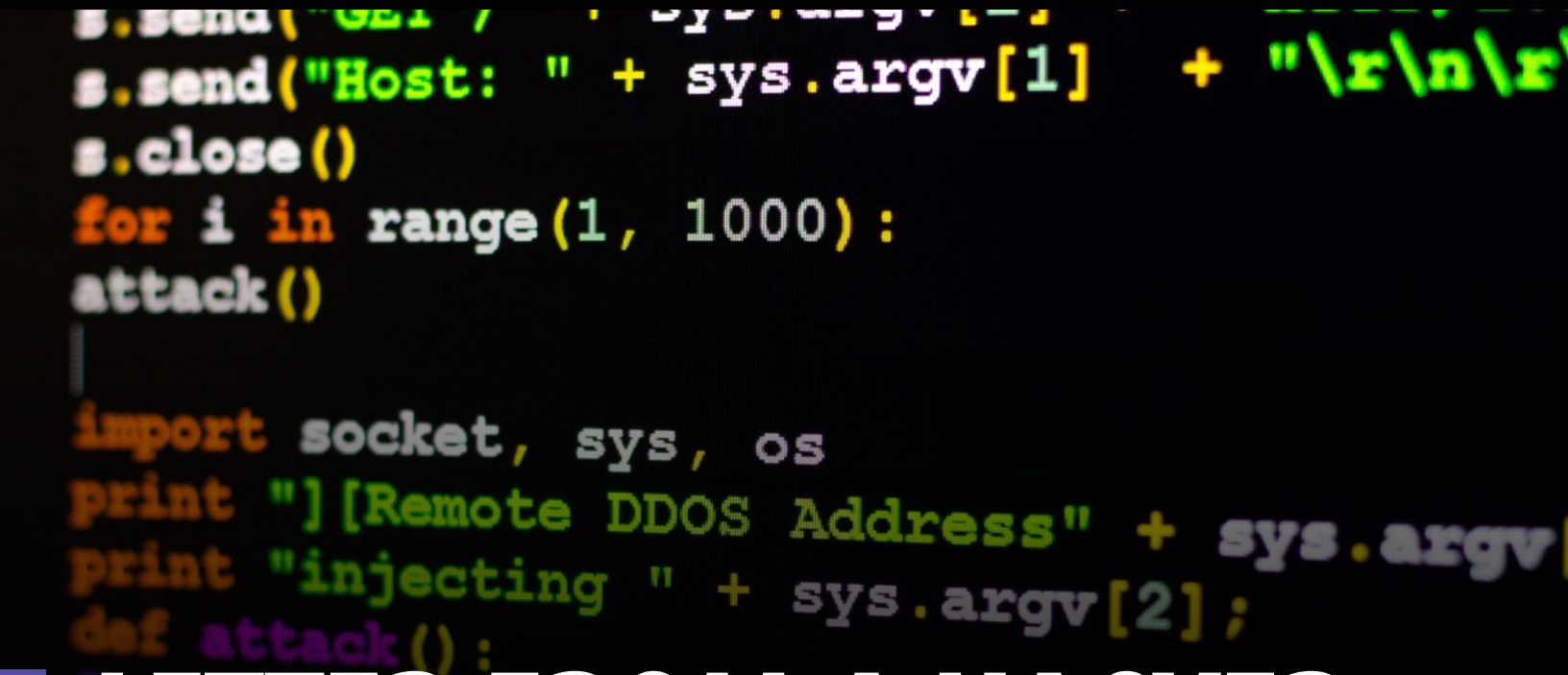
BUSTING THE ENTERPRISE RESPONSIBILITY MISCONCEPTION

With more and more functions being offloaded to the cloud, it is easy for vital security functions to fall between the cracks. End users believe that the IT department has everything under control and IT thinks the cloud provider has taken care of it.

"IT departments need to wake up to the fact that it is their responsibility to secure data being sent to the cloud," says Ward. "Do your homework, know what level of protection cloud providers offer and make sure there are no gaps for cyber criminals to exploit."

Ward cautions that there is no point product or silver bullet to ensure your data is fully protected and the enterprise stays incursion-free. It takes an integrated and automated system that protects data regardless of the device, application or network location.

"As the network perimeter continues to expand, automation is essential if security is to scale effectively," says Ward.



LETTER FROM A HACKER: THE NEW FRONTIER OF THE IoT

THE INTERNET OF THINGS IS WONDERFUL, AND IT'S GOING TO BE A HUGE OPPORTUNITY FOR US.

Welcome to the (unsecured) Internet of Things (IoT). Companies are embracing Bring Your Own Device (BYOD) with open arms. Their device-laden employees plod to and from the office with app-loaded cell phones, smart watches, fitness bands and tablets ready to connect to your Wi-Fi routers.

What these well-intentioned-but-non-technical folk have little grasp on, is that these devices have blasted open a wild new frontier of exploitation for hackers like me.

WHENEVER SOCIETY GETS A NEW TOY, WE SEE A BEAUTIFUL DARK CLOUD OF EXPLOITATION FLOATING JUST AROUND THE CORNER

In the next 10 years, there will be more smart devices connected to the Internet than computers and mobile phones combined.

That makes the Internet of Things an exploding area of growth in consumer technology. It consists of connecting devices that you would never consider to be internet-enabled. Things like vending machines, digital signage, refrigerators and even cars. By embedding connectivity into these devices, much like you would connect a tablet to a 4G network, these devices instantly have a much broader and more useful life.

THE MORE THESE INFORMATION DEVICES COMMUNICATE, THE MORE BENEFITS THEY OFFER ME. I SHOULDN'T BE TELLING YOU THIS...

The sensors and platforms on connected devices were never designed (for the most part) to deal with people like me. With a traditional computer, I must work to breach encryption, intrusion detection and security event management barriers. However, these new devices don't have a traditional OS.

Most manufacturers use the same hard-coded crypto or HTTPS keys for all of their IoT devices. This means that if I can get into one device, it's possible to use bots to get into millions more. I no longer need to hack into the largest, most complicated and well protected networks to leave my mark.

Wait, it gets better. I don't need to build a bot to control an IoT device myself. All I have to do is visit a Tor-based market like Alpha Bay and buy one; and that's exactly how hackers brought down the web in September 2016.

THE MANUFACTURERS OF CONNECTED DEVICES PAY ZERO ATTENTION TO SECURITY

First, French hosting provider OVH was taken down by a Dedicated Denial of Service (DDoS) attack from a botnet called Mirai. Mirai's bots took control of 152,000 compromised CCTV cameras and instructed them to send requests to OVH's servers in a record-breaking DDoS attack that reached server bandwidth volumes of 1 Terabit per second (Tbps) – a new world record that completely shut down OVH and all the websites they host.

Then, in early October, a seller named loldongs posted an offer of 100,000 bots on Alpha Bay for $7,500 and boasted, "I can take down OVH easily." don't know yet - but if Mirai was up for sale recently and this hack looks like Mirai and it acts like Mirai... I'll leave that assumption up to you.

In early October, a seller named loldongs posted an offer of 100,000 bots on Alpha Bay for just $7,500.

http://www.forbes.com/sites/thomasbrewster/2016/10/23/massive-ddos-iot-botnet-for-hire-twitter-dyn-amazon/#3ef826d6c915

The infrastructure needed to handle a 1Tbps volume data doesn't exist yet. In fact, the Institute of Electrical and Electronics Engineers (the people who develop the standards for Ethernet networks) predict that 400Gb/s will become available in 2017, and 1Tbps should come out by 2020.

A few days later, Twitter, Amazon Web Services, Netflix, Spotify and other major web companies reported major outages experienced by their customers across North America. Was it Mirai? Did someone take down a handful of internet behemoths with an army of brainwashed IoT devices they purchased on the Dark Web? We

WHEN'S THE LAST TIME YOU CHANGED THE PASSWORD ON YOUR HOME ROUTER?

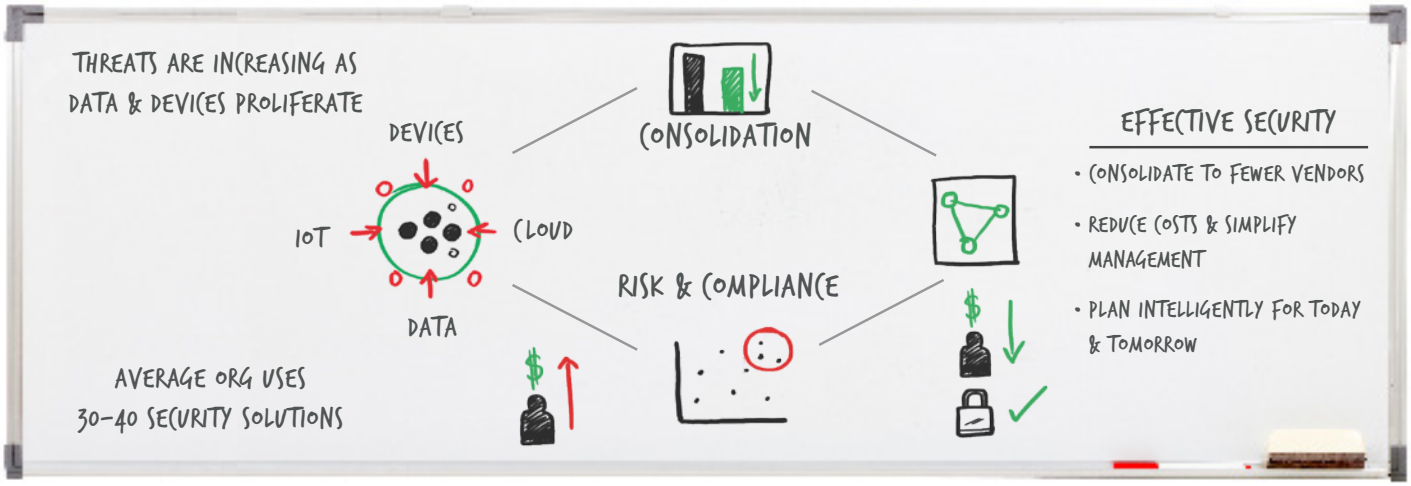
What the majority of people need to understand is that the majority of IoT devices can and will get hacked by people like me. I don't want to hack you in particular, I just want to borrow the computing power of your device for a while... And once I'm finished with it, I'll sell it to someone else. Right now, this type of hack is so easy that I'd like to help you level the playing field...

First, and foremost, read the *&%^ manual of your connected device. It contains instructions on how to lock the device down. And take its advice on creating a strong password. Second, delete the apps you no longer use, and update the ones you do. Do that right now. Third, don't rush through app and device set up prompts. You should understand what data is being collected, and how it's being used. Lastly, use Google to search for recent hacks or vulnerabilities in your product, and make sure to include the manufacture date, batch number and software version.

I've already said too much. But I'll leave you with this thought: As manufacturers create more advanced and connected technologies, ask yourself one thing: do you trust them?

Improve Security. Simplify Management. Reduce Costs.

Security Consolidation Assessment



Business Challenge

To address the latest threats, you continue to invest in new security solutions to protect your data. Yet adding more and more security vendors ends up costing your business money while not necessarily making you more secure.

Many organizations have 30 to 40 independent security vendors operating in their environment. And with internal resources stretched thin, finding the time and expertise to take inventory and develop a more cohesive strategy is simply beyond reach.

How This Affects You

- **Increased Costs** – spreading security investments across vendors minimizes your ability to leverage volume discounts and likely means you are paying for redundant features.
- **Increased Complexity** – having too many security vendors increases the time and effort required to manage these systems effectively, increasing strain on personnel.
- **Increased Risk** – a patchwork approach means leveraging solutions that aren't designed to work together holistically, creating potential gaps in coverage.

Customer Success Story

A Canadian-based life insurance company had eight unique security vendors in their environment. Costs were creeping up and internal IT staff were struggling to leverage the different management consoles.

Softchoice recommended the Security Consolidation Assessment to reduce the overall number of security vendors by standardizing on vendors that represented the largest portion of their overall security investment.

Softchoice's Consolidation Assessment resulted in:

- Simplifying management by reducing the number of security management consoles from 12 to 2
- Improving security by leveraging vendors designed to work effectively together
- Realizing savings of 45% compared to their previous year's security budget

According to PWC, in 2015:

24% - amount security **budgets** increased
38% - amount security **incidents** increased

- PWC 2016 Global State of Information Security Survey

>> Learn More <<

Book your assessment at the Ultimate Security Hub

softchoice

Connect with us today. 1.800.268.7638 | www.softchoice.com

@softchoice /softchoice company/softchoice