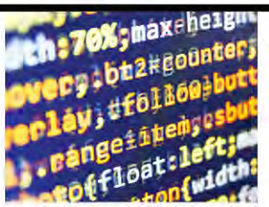
Data Security

Reformed con man **Frank Abagnale Jr.**, author of "Catch Me If You Can," talks about security in the Digital Age.

DISCOVER
what businessman Robert Herjavec has to say about keeping your company's data secure

BROWSE
more stories online, including security risks surrounding your social media

Cloud Tech
Learn why Kevin O'Leary thinks every company should make the most out of data on the cloud. **Page 6**



Know Your Enemy
Read up on what you need to know about ransomware and ways to protect sensitive information. **Page 10**

Hacker Tips
Get the inside scoop from famous reformed hacker Kevin Mitnick about how cybercrime really works. **Online**

The Essential Cybersecurity Guide to Protecting Your Business

As larger companies beef up their defenses, those who wish to steal sensitive data are taking advantage of smaller organizations lacking the resources to keep their digital assets secure.

Two-thirds of large businesses have experienced a data breach in the last year, and nearly half of small and midsized businesses have been the victim of a cyber attack. Many small and midsized businesses around the world are increasingly vulnerable to cyberattacks.

With the increase in cyber breaches, the National Institute of Standards and Technology (NIST) established a framework in 2013 for reducing risks to the nation's critical infrastructure. The framework takes a best practice approach to analyzing and mitigating risks, and recommends steps that any sized company can take for addressing cyber threats. All businesses should focus on creating a culture of cybersecurity and keep protecting the company top of mind for employees.

Outlined below are NIST framework best practices and general practices that any business can use to improve their online safety.

1. Identify your assets
Inventory your most valuable assets, the "crown jewels" that are of greatest importance to your business and would be most valuable to criminals, such as employee, customer and payment data.

2. Prepare protective measures
Assess what protective measures you need to have in place to be as defended as possible against a cyber incident.

Michael Kaiser
Executive Director, National Cyber Security Alliance

3. Detect problems
Have systems in place that would alert you if an incident occurs, including the ability for employees to report problems.

4. Respond promptly
Make and practice an incidence response plan to contain an attack and maintain business operations in the short term.

5. Recover and continue
Know what to do to return to normal business operations after an incident or breach, including assessing any legal obligations.

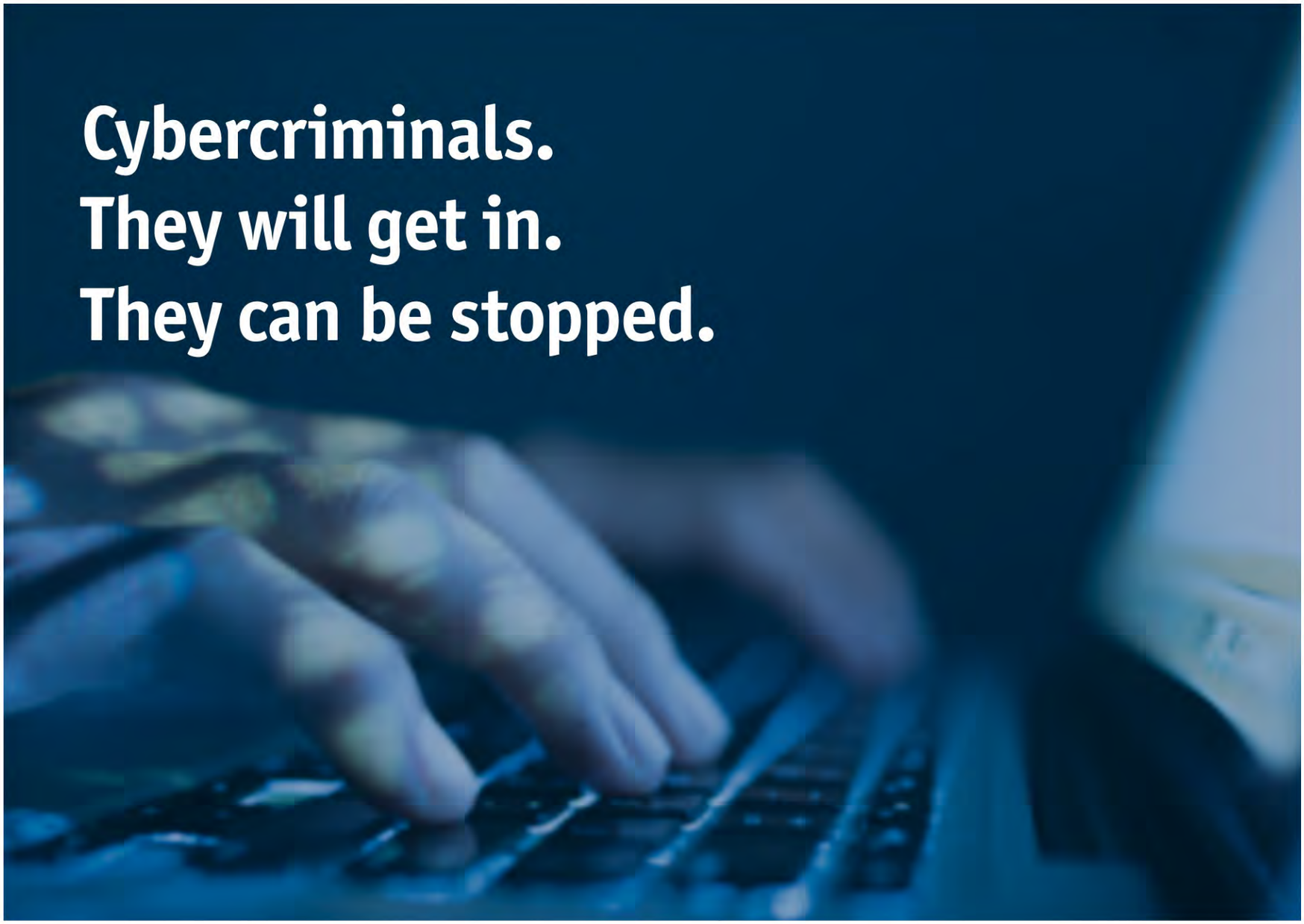
6. Keep a clean machine
Having the latest security software, web browser and operating system in your business are the best defenses against viruses, malware and other online threats.

7. Keep information safe
Secure accounts by adding two-factor authentication and making passwords long, strong and unique.

8. Protect the company's online reputation
Set security and privacy settings to your comfort level of sharing wherever you have an online presence.

9. Educate employees
Teach your employees basic best practices. For example, if an email, social network post or text message looks suspicious — even if you know the source — delete it. ■

Publisher **Luke Solomon** Business Developer **Jourdan Snyder** Managing Director **Luciana Olson** Content and Production Manager **Chad Hensley** Senior Designer **Kathleen Edison** Designer **Marie Coons** Copy Editor **Joey Jachowski** Production Coordinator **Tiffany Kim** Contributors **Frank Abagnale, Zoe Alexander, Michael Angelo, Steve Durbin, Michael Kaiser, Matthew Loeb** Cover Photo **Abagnale & Associates** All photos are credited to Getty Images unless otherwise credited. **This section was created by Mediaplanet and did not involve USA Today.**



Let us show you how.

The LogRhythm platform empowers your security operations team to detect and respond to cyberattacks – fast. LogRhythm can protect your organization from today's most advanced threats and help you stay one step ahead of cybercriminals.

See LogRhythm in action: **LogRhythm.com/demo-usa-today**

LogRhythm®
The Security Intelligence Company

5 Steps to Closing the Cybersecurity Skills Gap

Building a skilled cybersecurity workforce and increasing awareness around the career path needs to be a priority for companies that want to keep their data assets safe.

As technology advances and more devices connect to the internet, the potential for cyber threats is rapidly expanding. Unfortunately, the number of qualified cybersecurity professionals is not keeping up. A new study by ISACA and RSA Conference found that 6-in-10 cybersecurity team leaders say their staff can't handle anything beyond simple incidents, and they have often have trouble filling open positions with qualified candidates.

This information is cause for concern. These are the people responsible for protecting and defending their companies' most valuable assets. Here are five steps we must pursue to begin closing the cybersecurity skills gap.

1. Drive awareness of the cybersecurity career field.
Students are exposed to a number of careers from a young age, but being a cybersecurity practitioner isn't usually one of them. When students are aware of the job, the role models they see in those positions are overwhelmingly men. We need to equip guidance counselors and teachers with more information on cybersecurity careers and the benefits they offer — from the impact cybersecurity professionals have on organizations and the roles they play in safeguarding infrastructure, data, people and society to the above-average salaries they can command.

2. Help college students develop strong foundational cybersecurity knowledge.
University programs need to provide the knowledge and skills for cybersecurity jobs. Their courses should give a strong foundation of cybersecurity knowledge in their courses, but they can't stop there. Students must be given the opportunity to build hands-on skills throughout their college careers.

3. Focus on skills-based training.
Companies are looking for cyber professionals who don't just know what a threat is, but also how to detect threats, mitigate their effects and use their skills to guard against future threats. They want proof of the kind of skills best built in lab environments where individuals can respond to real threat scenarios. When you're protecting the data for thousands or millions of individuals, learning on the job just won't cut it.

4. Invest in the workforce.
To accomplish the shift from knowledge-based learning to skills-based training, organizations need to invest in their workforces. This type of training can be more expensive, but the outcome is exactly what companies are seeking — experienced cybersecurity professionals.

5. Open additional pathways to cybersecurity careers.
Four-year degrees in cybersecurity or related fields are excellent. However, we need to open additional pathways to industry in order to widen the talent pipeline. This might include a shorter technical school program or investing in training to bring staff from unrelated business units into the cybersecurity function.

The U.S. Bureau of Labor Statistics says the demand for cybersecurity professionals will grow by 53 percent through 2018. Industry, governments, academia and nonprofits need to work together and aggressively focus on meeting this need. ■

By Matthew Loeb, CEO, ISACA

Kevin O'Leary on Bringing Customer Data to the Cloud

By Zoe Alexander

Kevin O'Leary lays out what you should know about integrating cloud computing strategies to improve relationships with customers.

Anyone who has called into a customer service line before knows that it can be an unpleasant experience. Often there is a huge discrepancy in what companies say they are delivering in customer service and what the customer receives on their end. So, it's a good thing that customers are becoming increasingly empowered in how they access and learn about the marketplace itself. Through social media and tools like online cost-compares, customers can see exactly how businesses do business. Because of this new transparency, businesses' customer service technologies are crucial to building — and keeping — their client base.

Engagement on every platform

One approach to improving these services is by increasing flexibility for the customer. How? Taking customer service to the cloud. For example, through cloud technology, companies can take services that were once restricted to the computer and provide the same services on every digital platform, thus improving business-customer engagement.

"The key of the cloud is to be able to access your data from anywhere, anytime," says Kevin O'Leary, prominent co-host and investor on "Shark Tank." With this flexibility, customer service and tech support can respond faster, and more efficiently.

"If you have a customer, regardless of geography, you can get a lot of profile data about the experience they're having with your product and service," explains O'Leary. "As you build that data, the value of that customer goes higher and higher for you."

This is where customer retention comes into play. The better equipped you are to provide service to a loyal customer, the more likely they are to stay with you. With the benefits associated to using the cloud, you can first attract them, but then, perhaps even more importantly, you can maintain the relationship, increasing the value of your business.

Elevate your standing

"There is no question that if you are able to score in the top quartile of customer service, quarter after quarter, the value of your brand goes through the roof," says O'Leary. This crucial aspect is somewhat new for businesses, as social media now provides customers with the ability to either praise and rave about certain experiences, or detail their negative reviews — all for other potential and current customers to read. However, businesses can also take advantage of the information provided by these conversations and adapt to the needs of their client base.

"When you launch something that is clearly not being accepted, or is being accepted, you need to know why," says O'Leary. "You definitely need to be monitoring this. The cloud lets you do that instantaneously."

Digest the data

To get the most out of the cloud and social media data management, the question becomes: Do businesses need to invest in analytic solutions or can they just rely on a database which provides access to user data on the go? According to O'Leary, "It's not just enough to collect the data. You have to actually be able to manage it and get useful information from it." For this, there are multiple dashboards available to cut and review data in multiple ways to maximize benefit. "Having data and not having the ability to analyze or manage it is useless." ■

Discover a Better Way to Detect & Respond to Threats Before They Impact Your Business

AlienVault® Unified Security Management™

SC MEDIA LAB APPROVED

ASSET DISCOVERY & INVENTORY

VULNERABILITY ASSESSMENT

INTRUSION DETECTION

BEHAVIORAL MONITORING

SIEM & LOG MANAGEMENT

One Solution to Replace the Rest

AlienVault® Unified Security Management™ (USM™) is an innovative approach to security monitoring, delivered in a unified platform. The USM platform includes five essential security capabilities that provide resource-constrained organizations with everything they need for effective threat detection, incident response, and compliance, in a single pane of glass.

Designed to monitor cloud application and on-premises infrastructure, AlienVault USM significantly reduces complexity and deployment time so that you can go from installation to first insight in minutes. AlienVault is trusted by over 5,000 customers world-wide.

www.AlienVault.com/USAToday

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2017

THE CHANNEL CO. CRN SECURITY 100 2017

Forbes 2016 THE Cloud100 WORLD'S BEST CLOUD COMPANIES BESSEMER VENTURE PARTNERS salesforce ventures

3 Reasons Passwords Are Not Your Friend

Famous con man-turned-security consultant Frank Abagnale Jr. explains why data security norms are outdated and insufficient.

By Frank Abagnale Jr.

PHOTO: ABAGNALE & ASSOCIATES

When I was in my teens, it was a challenge to masquerade as someone else. It required that I forge the forms and credentials — even secure the proper costume. And all of this had to be done by hand and in person. In the last decade, fraud has changed; it's entirely online. It is phenomenally easier to pretend to be another person when you're behind a computer screen. All I need is your username and password. Over the past 60 years, the tools that criminals use have migrated online and have gotten more sophisticated, while the biggest form of protection has remained stagnant. The static combination of a username and password is extremely easy to replicate and replay, giving criminals easy access to the important information stored online. Passwords are simply insecure. So why do we continue to use them?

1. Passwords are outdated.
Despite the fact that the digital world and the criminal attacking it are progressing, username and password technology has not been significantly updated since they were invented. We wouldn't stand for a lack of innovation in any other industry, why do we do so when it comes to security?

2. Authentication does not equal identification.
In recent years, companies have been adding additional hurdles to username and passwords; however, these solutions, which include security questions, CAPTCHAs and company-issued tokens, are a hindrance to users and still do not verify the true identity of the consumer behind the screen.

3. Static information is our worst enemy.
Today the number one enemy lives within our devices in the form of malware. This nefarious technology "listens" to the information transferred from our devices and has the ability to "replay" this information to any relying party and gain access. Therefore, to avoid unauthorized access, organizations must consider dynamic methods which cannot be taken over by criminals in person or online.

Recently, the industry began to realize passwords are not the solution to protect information assets. Technology leaders are experimenting with logins that don't use passwords, and startups like Trusona are going a step further by not requiring usernames nor passwords. We need to see more companies taking action against passwords in order to better protect their customers and their bottom line. ■

Learning How to Navigate Data Security

We sat down with business luminary Robert Herjavec to discuss what data security means in a digital world.

You have an innate passion for data security, what was your earliest source of inspiration to get involved in this industry?

Robert Herjavec: I've been in this industry for over 30 years — long before there were headlines about security breaches and risk in the media every day. It was a growing space, even back then and I was simply looking for work. I was fascinated at the time by how security was adapting to business need and not leading business transformation. Now it's 50-50. A lot of our business is driven by compliance.

What was the most important lesson someone taught you about protecting your business and financial information?

It's the same lesson that helps me drive my business, which is that only the paranoid survive.

In the cyber industry we love to use this saying: "It's not a matter of if you will be breached, it's when you will be breached." It's not a fear tactic, it's just reality. It's important to never rest on your laurels. Always be planning, patching and updating systems. Understand your data, your access controls and your scope. Be paranoid.

What are your top data protection tips?

Train your staff on how to spot potential cyber threats, especially considering ransomware is often spread through online phishing campaigns. You also want to ensure that all data is backed up at regular intervals and is kept off the internal network. Make sure that all software applications are patched regularly — 44 percent of attacks are often due to unpatched code that's two to four years old.

Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code can execute malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources.

Get the help of an expert advisor in security. You don't know what you don't know — and likely don't have the manpower to support the size of your organization's infrastructure. You can benefit from advanced data correlation and threat intelligence by engaging an expert.

What's the biggest mistake you see others make when protecting either their data or businesses?

In the personal space we often want things to be easy and we will forgo security. We will lean toward using easy passwords or use all the same passwords. Sometimes it's easier to just use open networks or public Wi-Fi. We might even do our banking at Starbucks — it's crazy. We have evolved significantly in the enterprise space in terms of understanding cyber risk and putting measures in place to protect our businesses, our employees and our customers, but we have a long way to go. Data is used as a weapon today, and we can't make a one-and-done investment and assume things will get better. This battle requires ongoing investment in technology, in training and constant monitoring.

Best advice for someone who believes they already have all the data security and protection tools they need?

I shake my head because there is no such thing as perfect security; only the paranoid survive. ■

3 Ways to Combat Fear and Doubt Surrounding Ransomware

Ransomware is a specific strain of computer virus that's been in the news. Take a look at commonly asked questions and learn how to protect yourself.

Everywhere we turn, we read stories crediting ransomware with everything from locking hotel guests out of their rooms to shutting down hospitals. Ransomware has created a situation of fear, uncertainty and doubt (aka FUD) not only in the business world but also in the general population. In order to combat FUD, we need to do three things: understand how you get ransomware, understand how it works and, most importantly, understand what you can do to protect yourself.

1. How do you get a ransomware infection?

Ransomware is a new twist on an old technology. This strain of computer virus has been around since the last millennium. The technology is well-studied and understood. Ransomware relies on the same technology and methodologies as traditional malware (i.e., viruses, worms and trojans). That is, viruses infect a file or system on a computer and cause it to try and infect other files or systems on that computer. Worms actively try to infect other computers on your network. Trojans are designed to trick you to run something that enables either a virus or a worm. Most of today's attacks take advantage of one of these mechanisms to deliver the actual ransomware. The mechanism to deliver the trojan, virus or worm can vary. But the key point to remember is this: You can get ransomware from email or simply from surfing the web. There are two common delivery mechanisms.

A phishing attack is a well-crafted mail message that encourages you to open an attachment or click on a link. The file or the link then starts delivering malware. If the mail message is specifically crafted to a specific company or individual it may be called a spear phishing attack.

A compromised or spoofed website resembles a well-known popular website. The spoofed website, in the past, would try to get you to enter a username and password for the web site it was trying to spoof. Today's spoofed website has evolved to include automatically downloading software, also known as a drive-by download.

2. How does it work?

Ransomware may not start running right after you accidentally download it. Very likely it will stay dormant until your system is not being used. Then it will attempt to contact a repository on the web and register your system. Once your system is registered, the ransomware will download an encryption key. From there it will start to encrypt your system. Some forms of ransomware will try to encrypt just your files (documents, pictures, music). Others will try to encrypt the entire disk (including networked drives). Either way, when it's achieved its mission it will present you with a message letting you know your system is being held ransom. At this point, your choices are simple. You can contact the FBI and see if they have a set of keys that you can use to decrypt your system, you can pay the ransom or you can attempt to restore your system from backups.

3. How can you protect your computer or network from ransomware?

Besides the obvious, such as doing your best to avoid phishing attacks and spoofed websites, there are numerous solutions out there that can be used. The key is to ensure that your anti-malware technology has a few key attributes. It should analyze files and look for command sequences (referred to as signature analysis). It should analyze your system and look for program or system level changes. Finally, it should monitor programs on your system to see if a program is doing something outside of the usual.

While each technique overlaps and ultimately can provide a very strong solution, the key is to have a solution in place before you get infected by ransomware or affected by FUD. ■

By Michael Angelo, CRISC, Chief Security Architect, Micro Focus

Q&A

Christine Marciano
CEO, Cyber Data Risk Managers

How to Keep Data Safe at Work and at Home

Mediaplanet spoke with cybersecurity expert Christine Marciano to talk data handling best practices.

What steps do you personally take on a regular basis to secure sensitive data?

Whether I'm working remotely, in my office, or out of the country, I'm diligent in making sure my internet connection is secure. When on the road, I never connect to public Wi-Fi to check my email or transmit sensitive client information as that bears too much risk for both myself and my cyber insurance clients. In addition, I use different passwords for every application I use.

What is the biggest mistake you see companies make?

Many companies are chasing the latest and greatest security tools and systems. This leaves too many open endpoints, as most of these systems cannot be seamlessly integrated in a way the company requires. Today, all it takes is one unprotected endpoint in "people, process or technology" that leaves companies openly exposed as a target for a cyberattack or data breach.

What should readers be looking for in a security provider?

Too often, the conversation on cybersecurity is predicated on fear, uncertainty and doubt. Look for a cyber security provider that has a high level of integrity and don't choose one at random. I'm often asked by clients for a referral to security providers, and have a trusted provider list that I use. With all of the cybersecurity technologies available today, companies should look beyond what technology to invest in and understand the positive effects of why they're investing in it.

Changing International Data Regulations in 2018

In 2018, countries across the world must begin meeting data security mandates set out by the General Data Protection Regulation – and non-compliance will be costly.

The General Data Protection Regulation (GDPR) officially goes into effect in May 2018 and will have an international reach, affecting any organization that handles the personal data of European Union (EU) residents. This most certainly includes U.S.-based organizations. The GDPR aims to establish the same data protection levels for all EU residents and will have a solid focus on how organizations handle personal data. The benefits of the GDPR will create several compliance requirements, from which few organizations will completely escape. However, organizations will benefit from the uniformity introduced by the reform and will evade having to circumnavigate the current array of often-contradictory national data protection laws.

Consequences of non-compliance

Most countries (including all EU nations) have established supervisory authorities to oversee the use of personal data. Supervisory authorities, including the United States' Federal Trade Commission, will be granted investigatory powers by the GDPR, allowing them to investigate any complaint that they receive through a variety of measures. Complaints may be received not only from the data subjects themselves but also from any organization or association that chooses to complain or has been chosen by a data subject to represent their interests.

If an organization is found to be infringing the requirements of the GDPR, supervisory authorities have a variety of corrective powers from which to choose. These include the ability to issue warnings and reprimands to controllers or processors, and also include far more substantial powers, which can compel an organization to process data in certain manners or cease processing altogether, as well as force an organization to communicate data breaches to the affected data subjects.

Preparing now

No organization that operates on a global footprint of suppliers can afford not to prepare for changes that will result from new GDPR compliance rules. The checklist of rules requires extreme preparation and responsibility all of which must shouldered by the organizations who cannot look solely to government or regulators for help.

For most organizations, the next year will be a critical time for their data protection regimes as they determine the applicability of the GDPR and the controls and capabilities they will need to manage their compliance and risk obligations. With reform on the horizon, organizations planning or already doing business in Europe should get an immediate handle on what data they are collecting on European individuals, where it is coming from, what it is being used for, where and how is it being stored and accessed.

In theory, an organization should have completed its GDPR preparations well before May 2018 in order to gain assurance from, and provide assurance to, third parties' requests. Data protection, legal and information security teams should plan for this task so that they are not overwhelmed with requests closer to the enforcement deadline. ■

Steve Durbin, Managing Director, Information Security Forum

Cyber Insurance

What Every Company Leader Needs to Know about Navigating the Process

Cyber insurance is the most complicated insurance policy in the history of insurance. With many insurance carriers offering standalone cyber insurance policies, companies have many options to choose from and must carefully conduct their due diligence when reviewing varying policies and coverage options.

Even with the wealth of cyber insurance information available today, many companies interested in cyber insurance are clueless where to start.

This article offers some ideas on how to begin the cyber insurance process, and several mistakes to avoid.

Let's set the agenda.
Bruce Cybermann, CFO of a $250M company is buying cyber insurance for the first time. Since cyber insurance coverages, policy wordings, conditions, and exclusions vary greatly from one policy to the next, Cybermann needs help deciphering the plethora of options applicable to his company.

Where should he start?
Cybermann seeks out an experienced cyber insurance broker to help him as he does not feel confident that his general insurance broker has the cyber insurance expertise he requires.He finds an experienced broker that specializes in cyber insurance, and partners with her.

During this initial stage of the cyber insurance process, Cybermann and his cyber insurance broker have several calls to discuss: his company's services and products provided; cyber and data security risks; data classifications; total data record counts; devices used (I.e. mobile, IoT, etc.); details on how the company trains its employees on information security; how the company protects and secures its data, networks and devices; and lastly, third-parties that have access to the company's network and data. Indeed, many other questions will be asked and additional information may be required.

This information helps Cybermann's broker best-position and communicate the above criteria to underwriters on the cyber insurance application. Once the application is completed, Cybermann's broker is able to leverage her cyber insurance expertise and approach cyber insurance carrier underwriters that will have a risk appetite for the company. Depending on the complexity of Cybermann's company, the broker may request a conference call be scheduled with underwriters to help further ascertain the company's cyber and data risk exposures.

Moving ahead, Cybermann is very concerned that he does not make any mistakes that will leave his company potentially uncovered. Rightfully, he is also concerned about his own position after hearing about other executives losing their jobs after a data breach happened on their time.

Cybermann asks his broker what mistakes others have made when purchasing cyber insurance.

Top 3 Cyber Insurance Mistakes to Avoid

1. Failing to work with an experienced cyber insurance broker. The complexity of cyber insurance coverages relates to the adage "you would not want go to your podiatrist for a heart problem." Therefore, going to a general insurance broker for proper cyber coverage is a huge pitfall. Fortunately, Cybermann understood the importance of seeking out an experienced cyber insurance broker right from the start.

2. Thinking that the company's D&O insurance policy precludes having to purchase cyber insurance. Some D&O policies include a "failure to maintain insurance" exclusion. While this is not a specific cyber exclusion per se, it can act much in the same way, precluding coverage for claims related to the failure to acquire or maintain adequate insurance.

3. Assuming it's covered. Cyber insurance is not a panacea. What you don't know—can hurt you. It is crucially important to review the policy coverages, definitions, exclusions and conditions and understand what's covered and not covered.

Please note, this is not a conclusive list as there are many other traps to avoid.

For help, please visit
http://www.DataPrivacyInsurance.com

Researching Data Security Tips and Tricks

	What steps do you personally take on a regular basis to secure sensitive data?	What is the biggest mistake you see companies make?	What should readers be looking for in a security provider?
 **Josh Feinblum** Vice President of Information Security, Rapid 7	Work to secure sensitive data never ceases. Sensitive data is impacted when we build new products, improve existing products, communicate with our customers or support our employees. My focus is making sure we're making continual progress and staying up-to-speed on high impact initiatives so we may avoid unpleasant surprises.	Many organizations build complex security programs and processes, and forget the basics. Getting back to fundamentals is the most valuable action companies can take. If they're investing in a security program and don't have a strong patching program or a widely-adopted approach to two-factor authentication, they're doing things in the wrong order.	A good security provider leads by example and should establish a relationship with you that feels like a partnership. Make sure they are securing your data the way you secure it yourself. It speaks volumes about an organization if they espouse one set of behaviors yet fail to follow their own guidance.
 **Matt Morris** Vice President of Products and Strategy, NexDefense	It's an inconvenience, but a little bit of pain daily can prevent major problems later on. Use passwords, preferably long ones, for everything. Leverage two-factor authentication and lock screen savers with passwords. Use secure virtual private networks (VPN), endpoint protection and virus scanning software. Be skeptical of links and attachments in emails and avoid USBs.	The biggest mistake I see industrial-leaning companies make is taking a reactive approach. Far too many companies wait till something like #WannaCry, #StuxNet, #Havex or a similarly deviant malware or attack shows up on their doorstep. Companies must be more vigilant and prepare themselves now.	Find companies who fundamentally understand a holistic view of production, safety and security. Many providers claim to assist with human errors, system failures or malicious security, but actually focus solely on security. This is at the exclusion of risks such as design flaws, system misconfigurations and regulatory issues.
 **James Carder** Chief Information Security Officer and Vice President, LogRhythm	When securing sensitive data, consider three aspects: data at rest, data in motion and the need to know. For data at rest, make sure the data is encrypted. When transmitting the data, make sure you use a secure transport mechanism that leverages encryption. Finally, only provide the data to people who need to access it.	The biggest mistake companies make is assuming they are not at risk of a cyberattack. These companies tend to not invest in keeping their information technology (IT) infrastructure modern. They don't enforce basic processes and principles such as patch management or backup and recovery, and don't have adequate security controls in place.	Readers should be looking for a security partner, not a provider. Readers should also be looking at security partners that are in alignment with their business needs. The best partners provide technology and services that have a substantial impact and value to the reader's overall security mission.
 **Nicholas Friedman** CEO, Templar Shield	Securing sensitive data goes hand in hand with limiting potential vulnerabilities through risk awareness. I encrypted data in transit and at rest, use VPNs when traveling, and only use secured wireless networks. Additionally, I keep my systems up to date on patches, avoid suspicious emails and rotate my passwords regularly.	Not knowing where their sensitive data lies and when to get rid of it. Too many times companies are just checking compliance boxes and not taking a risk-based approach to securing their data. This leads to applying under- or over-compensating controls which can cause additional costs to the organization.	A good partner won't sell you a tool or service to solve your security needs. They invest time to understand your business, grasp your maturity, identify weaknesses, and provide both strategic and tactical solutions to mature your security posture. Limiting potential vulnerabilities through risk awareness, management and mitigation is the goal.
 **Chris Pogue** Chief Information Security Officer, Nuix	I use full-disk encryption on my laptop; if it's ever stolen or lost, the data has a significantly less danger of disclosure. I encrypt all of my documents on a small USB drive and keep it separate from my laptop. I also back up critical data encrypted in the cloud, use a password manager that is both local and cloud-based, and use multi-factor authentication whenever and wherever I can.	Most companies don't understand the threats and oversimplify countermeasures. Many companies rely on legacy security tools, which are cobbled together and present security gaps. They operate with a limited view of activity across the enterprise, and mistakenly focus on external threats when insiders — inadvertently or otherwise — can pose a threat as well.	The key is to find a security vendor that will listen to you about your needs, demonstrates expertise, works with your existing IT and security investments, and is focused on your success. There are plenty of vendors trying to sell you their widget or solution, ranging from bad to good, but not all of them are focused on working together with you to safeguard your data, your systems and your customers.

REMOVE THE RANSOMWARE BULL'S-EYE FROM YOUR NETWORK

With the recent WannaCry cyberattack, ransomware is now in the spotlight. But what may not be on your radar is the role that DNS plays in cyberthreats. The majority of ransomware uses DNS to carry out attacks. So does most malware, hijacking, and data theft.

Infoblox locks down DNS and removes the bull's-eye from your network, and brings ransomware to its knees. Automatically, completely, and in real time.

Make DNS your first line of Defense.

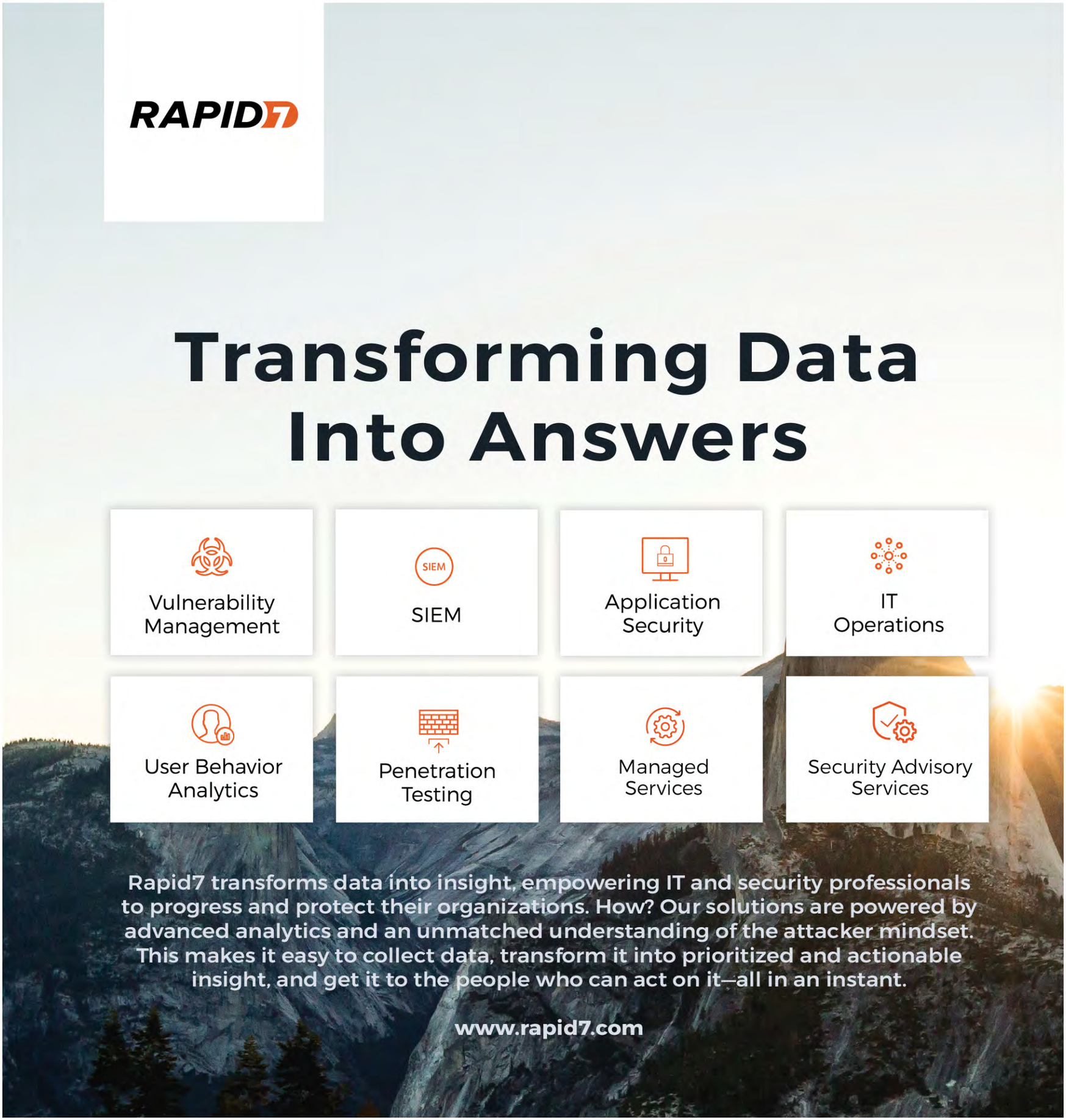
Infoblox®
CONTROL YOUR NETWORK

SECURITY. IT'S IN OUR DNS™

Learn more at: www.infoblox.com/threat-center

RAPID7

Transforming Data Into Answers



Rapid7 transforms data into insight, empowering IT and security professionals to progress and protect their organizations. How? Our solutions are powered by advanced analytics and an unmatched understanding of the attacker mindset. This makes it easy to collect data, transform it into prioritized and actionable insight, and get it to the people who can act on it—all in an instant.

www.rapid7.com