FEBRUARY 2017
VOL. 19 | NO. 1

INFORMATION SECURITY

IN 2017, ATTACKS WILL FOLLOW YOUR DATA

Cyberthreats: What's coming next, and how to prepare for it.

TechTarget

Mass Clouding

There's no turning back. Consumers and enterprises see the possibilities of cloud-based voice recognition systems; so does Amazon. BY KATHLEEN RICHARDS

CLOUD-CONTROLLED CARS? At CES 2017 in January, auto technology companies touted a future rife with seamless connectivity: Your car talks to your appliances, your smartphone applications interact with your dashboard and each cloud-based system is autonomous so that it can be set up to serve the individual's needs.

Ford is planning to roll out these features in some models such as the Ford Fusion as early as this summer. The company also announced a partnership at CES 2017 with Amazon involving the online retailer's Alexa Voice Service technology.

But cybersecurity has to catch up before much of what was showcased at CES becomes a reality. Or does it?

The reliance on cloud-based systems will enable attackers to find new ways to pose security threats, according to SANS Technology Institute's Dean of Research Johannes Ullrich, who writes about these risks and more in this month's cover story.

"Your car may not start until you pay off a ransom, or your door locks may not open until you transfer the right number of bitcoins to the attacker holding them hostage," said Ullrich, who also leads the research team at SANS Internet Storm Center.

The enterprise security implications from network-connected devices and one-off implementations of cloud-based systems, such as enterprise resource planning, will present numerous challenges. How can companies get out in front of these threats? Hear more about what's coming next and how to prepare for the creative ways that attackers will follow your data in our coverage this month.

Also in this issue, we talk to a financial services CISO whose role has expanded to include direction on cybersecurity products. Marcus Ranum continues his "how did you get here?" series with a chat with the head of global compliance for an e-commerce provider. Security expert Michael Cobb looks at early drafts of the National Institute of Standards and Technology Digital Identity Guidelines (NIST Special Publication 800-63-3) and offers tips on which password recommendations may make sense for enterprises. ■

KATHLEEN RICHARDS *is the features editor of* Information Security *magazine. Follow her on Twitter: @RichardsKath.*

CYBERTHREATS: HOW ATTACKS WILL FOLLOW YOUR DATA

You can move your data to cloud-based systems and web services, but you can't hide it there. Hackers and predators have more ways to find it.

By Johannes Ullrich

IT IS ALMOST certain that your social security number has been leaked in a breach. There's also a high probability that at least one of your credit card numbers will fall into the wrong hands over the next 12 months.

In the past, attacks to steal such data represented lucrative and sustained criminal enterprises. But due to the abundance of stolen data, the value of individual records has plummeted, and many stolen records never get used.

Criminals have had to find new ways to monetize their skills. They have turned to ransomware to increase the value of the information by selling it back to the victim. Now it's not just your identity at risk, but important business documents and, in some cases, critical medical data.

Future attacks will combine many of the patterns we have seen recently, and criminals will continue to automate these attacks. They have already started taking advantage of the expanded use of network-connected devices and cloud-based systems to find new ways to threaten information security. Many industries increasingly depend on network-connected devices to regulate everything from manufacturing to delivering products.

Up to now, most of the attacks against these systems happened accidentally. The few intentional attacks documented so far are attributed to nation-state actors with resources and insight into the communication protocols these systems use.

HOLDING IoT DEVICES 'HOSTAGE'

But like sophisticated techniques well-funded groups have used in the past, even attacks against industrial control systems will become commoditized. As tools and methodologies behind these attacks spread, less-skilled hackers will be able to launch ransomware attacks against these systems. These malware attacks will hold the systems hostage, threatening to stop or destroy manufacturing facilities until the victim pays a ransom.

In everyday life, similar systems are used and susceptible to these same cloud security threats. Your car may not start until you pay off a ransom, or your door locks may not open until you transfer the right number of bitcoins to the attacker holding them hostage. With faster ways to find vulnerable devices, and by using existing compromised devices as a bridge into vulnerable networks, it will be up to the creativity of the attacker to find ways to turn the internet of things (IoT) against us.

Home automation is one area where the internet of things is exploding, and standards for control of these systems are starting to emerge. With standardization, the products become not only more attractive to consumers who look for interoperability between different devices, but also to attackers who can use standard communication APIs to attack these products. Research into home automation often focuses on insecure wireless communication protocols. But while attacks against these protocols require physical proximity, much of the cloud-based control infrastructure of these devices is remotely accessible and just as vulnerable to cloud security threats.

Many devices in home automation and alarm systems use cloud-based systems to communicate. The smart home device will regularly send status updates to the cloud server and retrieve new commands to execute. Weak and incorrectly implemented authentication between device and cloud is often the failure point that can be exploited to either attack the cloud infrastructure or the device. For instance, a simple distributed denial-of-service (DDoS) attack against a cloud service controlling thermostats can disable them and in colder climates may cause substantial damage. Some of these attacks have also been demonstrated against modern cars that rely on cloud-based services to communicate with mobile applications used to remotely start a car or open doors.

IoT attacks also have the possibility to be more destructive. So far, devastating attacks are not common and are mostly limited to DDoS attacks, which do not cause permanent damage. But future attacks, if they are combined with ransom demands, may very well destroy

(Continued on page 7)

Timeline of Internet-Connected Attack Paths

DECEMBER 2014: A phishing attack on an unnamed German steel mill enables hackers to take control of the plant's network and production systems. Failure to shut down a furnace properly results in serious damage, according to the German Federal Office for Information Security.

OCTOBER 2016: DDoS attacks involving the Mirai botnet made up of internet-connected devices—routers, CCTV cameras and DVRs—flood Dyn servers with DNS lookup requests of IP addresses. Major North American and European companies' websites and services are disrupted for hours. According to security blogger Brian Krebs, Mirai code was available as open source weeks before the attack.

2008 2014 2015 2016

AUGUST 2008: Hackers allegedly sabotage surveillance cameras and sensors in a 1,099 mile Baku-Tbilisi-Ceyhan oil pipeline designed to circumvent Russia. Alarm systems fail to trigger when the section in Refahiye, Turkey, explodes.

NOVEMBER 2015: Hackers infiltrate Target's networks using stolen credentials from the retailer's HVAC vendor and gain access to personally identifiable information of 70 million customers.

MARCH 2016: A phishing attack allows hackers to pursue a months-long effort to infiltrate a Ukraine power grid and take its substations offline. Remote access to SCADA systems and over-writing of firmware are steps that facilitate the attack.

SOURCE: PIPELINE: LEONID IKAN/FOTOLIA; STEEL MILL: SINGKAMC/ISTOCK; TARGET: ANTHONYROSENBERG/ISTOCK; POWER GRID: HEIBAIHUI/ISTOCK; DDOS: BRIANAJACKSON/ISTOCK

(Continued from page 5)

devices intentionally or not. Most IoT devices allow a remote user to upload new firmware, which can then be used to disable the device permanently.

EXPLOITING DEPENDENCIES ON WEB SERVICES

Software developers have been aware of the dangers of using insecure components in software development for a while now. Modern software tends to rely on large, complex libraries, and much of it is written by just combining these libraries in new and innovative ways. But vulnerabilities in a commonly used library can affect many different software packages. If developers don't carefully track these vulnerabilities and release updates for patched components, software can remain vulnerable long after a flaw has been disclosed and fixed in a library.

With the emergence of cloud-based microservices, this problem will only become worse. Instead of including a library in software shipped to clients, the software now relies on cloud-based web services to perform certain functions. The developer and the end user depend on these services, which they do not control and have no ability to audit. A compromise of a web service may go unnoticed for a long time, and the attacked service could provide "bad data" to try to manipulate business decisions. This data modification problem is an increasing risk among cloud security threats and hard to detect.

The reliance on cloud services is also worrisome for authentication and access control decisions. An attacker who is able to identify a flaw in a popular authentication service could easily use it to access a wide range of services that depend on its integrity. OAuth, a very popular standard to authenticate to cloud services, is often implemented incorrectly and subject to phishing attacks. While two-factor authentication is becoming more popular with these services, it is still not universally implemented. Often, web services that require two-factor authentication for interactive logins provide workarounds for systems that have to connect to the service without user interaction. Web-based email services had a difficult time implementing two-factor authentication while at the same time allowing automated polling for new messages from various mail clients. An attacker who can compromise a user's credentials is often able to configure an API key, or application-specific password, that can be used to access the service well after the intrusion was identified and the primary password for the account was changed.

MODIFYING CLOUD DATA

But compromised cloud services can go much further. In recent years, enterprise resource planning (ERP) systems have become an attractive target for more sophisticated attackers. These attacks are either attempts to extract proprietary information from these systems or they're attempts to affect business decisions by manipulating data. The complexity of the systems, and the fact that most are

one-off implementations for a company, makes it challenging to monitor and secure them. Each implementation is different, which makes it difficult to apply generic hardening guides like the ones used for commodity software, web servers and databases.

Recently, more and more of these systems either use cloud-based web services to interact with suppliers and customers or the system itself is migrated to a cloud platform. Compared to on-premises ERP software, a cloud system is typically offered using the software-as-a-service (SaaS) model, which removes expensive upfront cost and leaves most of the maintenance and security responsibility for the system with the vendor. Authentication and access control have to be correctly integrated with the SaaS provider's systems. The security practices the SaaS provider follows will in the end affect the security of the data stored in this system.

But at the same time, these vendors are now becoming an attractive target. A compromise of a vendor can provide access to data for many different companies. Such a compromise could come from insiders at the vendor. Vetting employees who have physical access to the data in data centers is now up to the SaaS provider, not the company owning the data.

Organizations need to continue to learn to detect cloud security threats and react to them faster. Large enterprises need to learn to close the loop and apply internally sourced threat intelligence quickly. Disseminating current and relevant information to IT and security operations is more important than ever.

At the same time, the network environment is changing. Servers will migrate to the cloud, and the network they connect to will no longer be controlled by the organization's security staff. Instead, more and more control devices will enter the corporate network.

These devices will expect connectivity to the cloud-based infrastructure and can no longer be "air-gapped" to mitigate attacks. Interactions between different network segments will become increasingly complex. Network segmentation, which is often used to mitigate the threats from devices, will no longer be practical if radio frequency ID scanners in a warehouse need to interface with a cloud-based inventory management system or an e-commerce platform that uses a content delivery network. Whitelisting of IP addresses and designing a network with strict security zones and enclaves will become a lot more challenging. ■

JOHANNES B. ULLRICH, *Ph.D., GNFA, GCIA and GWEB, is the dean of research at the SANS Technology Institute and director of the Internet Storm Center. Follow him on Twitter: @johullrich.*

FICO ENLISTS CISO IN SECURITY PRODUCT DEVELOPMENT

As head of FICO's information security program, Vickie Miller's role is wide-ranging.

By Alan R. Earls

LENDERS HAVE RELIED on FICO ratings to assess future credit risk for decades. Vickie Miller, in her role of CISO at the San Jose-based data analytics company, has spent years managing cybersecurity and privacy risk as the head of its information security programs. A Certified Information Systems Security Professional and Certified Information Privacy Professional, Miller received the ISE Central Executive of the Year Award 2015 from T.E.N., a national tech exec networking organization. Recently, for a time, she also served as senior director of cybersecurity product management at FICO.

Miller has also made her mark beyond financial services. She is an executive board member of InfraGard, a partnership between the FBI and the private sector, which works to share information and intelligence in an effort to prevent hostile acts against the United States. As an extension of that program, she works with the FBI Citizens Academy, which involves individuals in leadership roles—ranging from CIOs to ministers—in information sessions and discussions about law enforcement, national security challenges, protecting intellectual property and

more. "As part of that, I was even invited to a program at the FBI academy at Quantico, Va.," Miller said.

While Miller continues to focus on keeping FICO secure, she also offers input and advice to company teams involved in creating security-related products.

"We are the subject-matter experts because we are the ones that stare at the screens, so we have a voice in seeing how the tools are developed, which is a little novel for my team," she said. Alan R. Earls caught up with Miller to ask her about the changing role of CISO as information security programs are recognized as a business requirement.

How do you see the role of CISO evolving?

If you look back at the past decade or so, there have been an increasing number of CISOs being appointed at companies across all industries, which is a great thing. The ROI of having a CISO is clearly demonstrable. I have seen statistics that indicate that losses from cyberattacks at companies with a formal information security program and with a person in charge of it are significantly lower than at other organizations.

FICO has always had a security focus because we serve the financial services sector, but more and more companies are [adding the role of CISO] and institutionalizing their information security programs. The Target breach led to liability for directors. Widespread visibility into that situation has encouraged a lot of publicly traded companies to invest more money in security and in terms of

Vickie Miller, VP and CISO at FICO

elevating the issue across the company. A CIO must be more understanding of risk and data privacy. What I have found personally is that I love the nitty-gritty operational and tactical things, the hunting and adversary work. But I do less and less of that as I have learned that you must

become an ambassador for what needs to happen within a company to keep it secure. You need to communicate about risks and how to mitigate them. The business must know that security is inherent to what we do. You can't just say so; you must elevate an understanding of the ramifications surrounding security and engage people in making improvements.

What is your focus these days at FICO?

It is wide-ranging. There has not been a day I can think of at FICO where something new, different or interesting didn't happen. It might not be exciting, per se, but it is very stimulating to work in an environment that requires a certain breadth of knowledge. You must have diplomatic skills and a sort of thick skin and a tolerance for fatigue. But I think of some people who find themselves in jobs where they say they are bored. I can't imagine ever being bored. Some would look at this work and say that all you are doing is looking for anomalies and alarms. I must tell you some of the developments in tools are very interesting. There are a lot of opportunities to hunt for things, and there is always an adversary out there.

Is there a key to staying on top of your game in the role of CISO?

I would say there must always be a passion for learning and often for displaying Myers-Briggs type ENTJ [extroversion, intuition, thinking, judgment] characteristics. ■

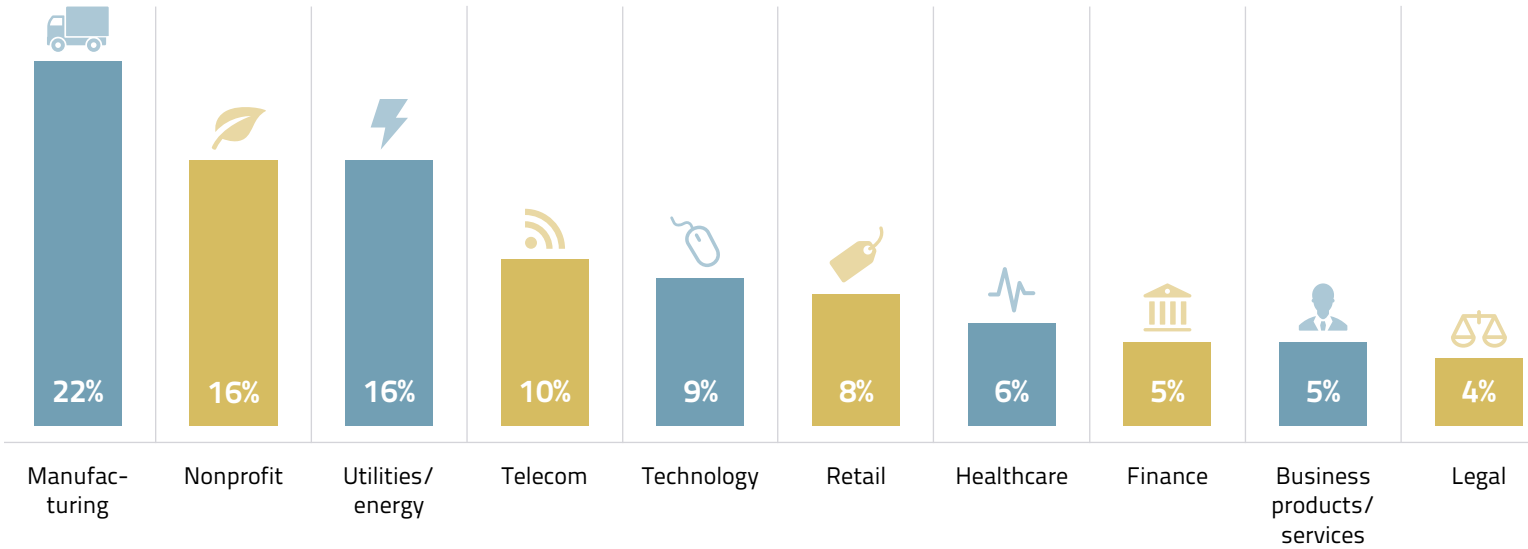
ALAN R. EARLS *is a Boston-based freelance writer focused on business and technology.*

Ransomware Attacks Doubled in 2016

With high sums paid, ransomware gets all the attention. But it's still a fraction of total malware, a new report shows, and not the only way criminals gained control of enterprise systems. BY KATHLEEN RICHARDS

Where Software Attacks

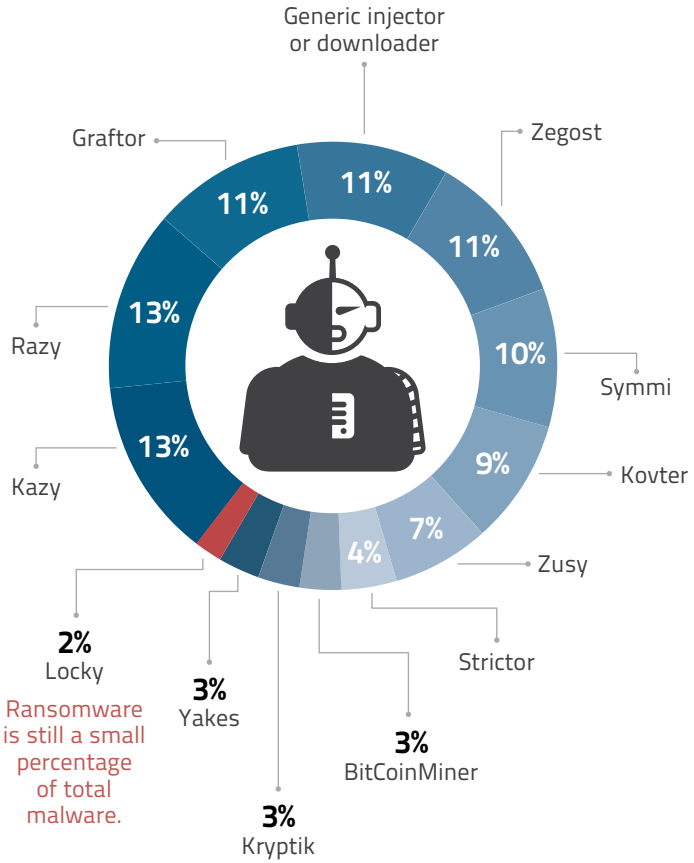
Percentage of total malware by industry



SOURCE: CARBON BLACK THREAT REPORT, DECEMBER 2016; NUMBERS HAVE BEEN ROUNDED

Families to Watch Out for

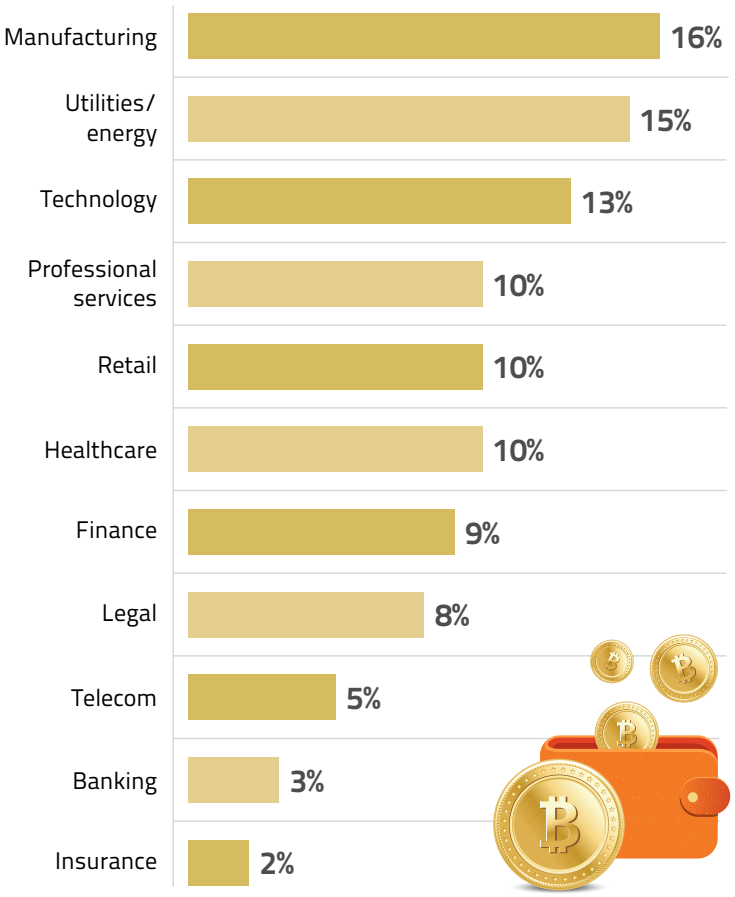
Percentage of malware by identification



SOURCE: CARBON BLACK THREAT REPORT, DECEMBER 2016; NUMBERS HAVE BEEN ROUNDED;
ART: JORGE REYES, HTTPS://CREATIVECOMMONS.ORG/LICENSES/BY/3.0/US/

'That'll Be Thousands of Please'

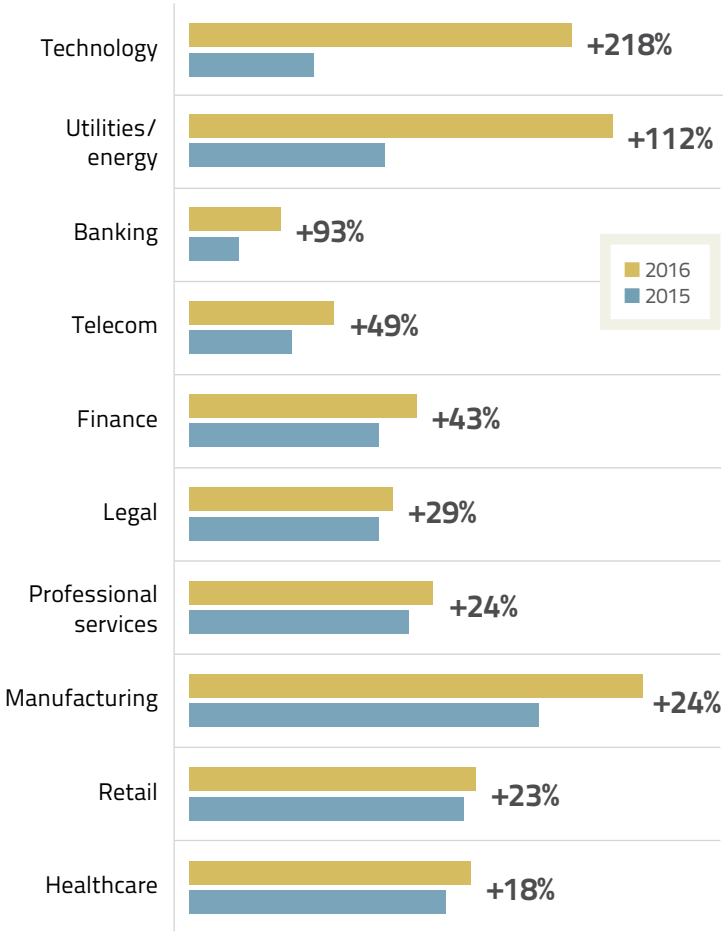
Total ransomware by industry



SOURCE: CARBON BLACK THREAT REPORT, DECEMBER 2016; NUMBERS HAVE BEEN ROUNDED;
BITCOIN ART: DIBRONZINO/FOTOLIA

Targeted More in 2016

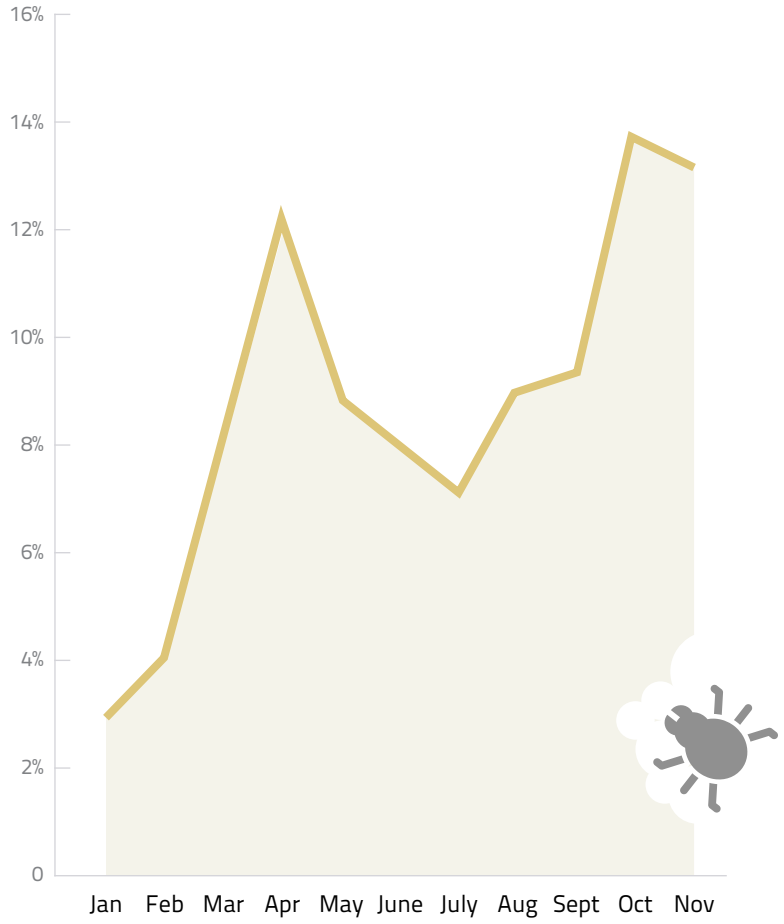
Year-over-year ransomware growth by industry



SOURCE: CARBON BLACK THREAT REPORT, DECEMBER 2016

Rise in Attacks Beyond Malware

Microsoft PowerShell and WMI-based attacks in 2016



SOURCE: CARBON BLACK THREAT REPORT,DECEMBER 2016; WMI STANDS FOR WINDOWS MANAGEMENT INSTRUMENTATION

WHAT NEW NIST PASSWORD GUIDELINES SHOULD ENTERPRISES ADOPT?

NIST is coming up with new password recommendations for the U.S. government. We cover the most important changes.

By Michael Cobb

THE NATIONAL INSTITUTE for Standards and Technology, or NIST, is creating new guidelines for password policies, which will be adopted by the U.S. government. The Digital Authentication Guideline is up for public preview on GitHub's and NIST's websites. What are some of the significant changes in NIST's recommendations? Should enterprises consider adopting these password recommendations?

Many enterprises and online services are looking to replace the much-maligned password. Several financial service companies, for example, are rolling out biometric authentication options for their customers, and Google offers the option of two-factor authentication, where a verification code is sent to a user's mobile phone.

However, there's still no universally accepted alternative to the password. So, despite its weaknesses, both in terms of security and practical use, many systems rely on it—even if only as a fail-safe for when a user's fingerprint or voice can't be correctly identified. Since passwords are here to stay for a while longer, it's refreshing to see research by NIST looking at how to make password

authentication more robust and more user-friendly.

NIST has been studying how passwords are created and used in order to produce more effective password recommendations and policies. Special Publication 800-63-3: Digital Authentication Guidelines is still a work in progress, but it already proposes some significant changes to what has long been accepted as best practices; as it turns out, some of them don't actually improve security.

USER-FRIENDLY POLICIES

The overriding principle behind the NIST password recommendations is to make password policies user-friendly, as arduous password rules end up being circumvented or ignored by users and support desks, negating any possible security benefits. Many users have the same password for several sites, so an employee's eight-character-long, complex work password can be vulnerable if it's used for their online banking and social media account logins as well.

It's not surprising that one of NIST's first password recommendations is PINs should be six digits long and passwords should be a minimum of eight characters, with a maximum length of 64 for more sensitive accounts. Remembering a password longer than eight characters is not necessarily easy, but NIST's new guidelines allow the use of all printable ASCII characters and all Unicode characters, including emojis, to improve usability and increase variety. Combine this with the recommendation that users should be encouraged to create longer phrases instead of hard-to-remember passwords or ones based on character swaps, such as *pA55word*—which may appear complex, but, in fact, are not—and it opens the way for long, complex and easy-to-remember passwords.

NIST's new guidelines allow the use of all printable ASCII characters and all Unicode characters, including emojis, to improve usability and increase variety.

Also, passwords should no longer automatically expire after a certain period unless there's a good reason, such as they have been forgotten or there's suspicion they have been phished or stolen and could therefore be subjected to an offline brute-force attack. This would mean there has to be some form of monitoring in place to detect potential compromises. LinkedIn didn't know its password database had been compromised for years and, thus, had no reason to force users to change their passwords. But had users been made to change their passwords every few months, the database of passwords from 2012 would be useless to attackers.

There is also advice on how to store users' passwords

safely. All passwords must be hashed, salted and stretched when stored. This will dramatically reduce the ability of hackers to cost-effectively crack passwords either in bulk or individually. Systems also need to check new passwords against a dictionary of known bad choices. Administrators need to ensure this dictionary matches its users' most likely choices—which, depending on location and industry, may not necessarily exactly match the world's 100 most likely passwords. Having 100,000 such entries is suggested as a good starting point.

NO MORE HINTS OR SMS

While these guidelines may seem long overdue, the recommendation to do away with knowledge-based authentication (KBA), password hints and SMS codes is more contentious. KBA and password hints greatly reduce the number of costly and time-consuming password resets, but they provide little additional security, as was shown in Adobe's 2013 password breach and the fact that answers to KBAs are too easy to find on the internet. Also, NIST concludes that one-time passwords sent via SMS are too vulnerable due to mobile phone number portability, attacks like the SS7 hack against the mobile phone network and malware that can redirect text messages.

Any security control needs to continually evolve and adapt to how it is actually used in real life in order to withstand changing attack techniques and the constant rise of computing power. NIST's goal is to improve how users create and how systems store passwords, reducing unneeded complexity wherever possible. Indeed, Special Publication 800-63-3 will become compulsory for the whole U.S. government.

Enterprises should look at following these guidelines where practical, as they will quickly be considered best practices in the court of public opinion. Password length and complexity requirements can usually be changed relatively easily in most programs or through group policy, but changes such as eliminating SMS in two-factor authentication schemes won't be cheap or straightforward. Administrators will also need to implement an alternative account-recovery process if they choose to abandon hints and KBA. There's no obvious substitute other than a password-reset email, which can also be insecure if not implemented correctly. It will be interesting to see what the final password recommendations are. ■

MICHAEL COBB, *CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book* IIS Security *and has written numerous technical articles for leading IT publications. He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS).*

Security and Compliance With Digital River's Dyann Bradbury

Bradbury chats about her early interest in computers and the uncharted path to her role as head of compliance for a global payments company.

BY MARCUS RANUM

DYANN BRADBURY IS the senior director of compliance at Digital River, a global e-commerce technology provider that processes online transactions in Europe, China and South America. "My role is to build that trust between IT and compliance," said Bradbury, who joined the company, based in Minnetonka, Minn., in 2006.

She also served as president of the InfraGard National Members Alliance from 2009 to 2012. Bradbury chatted with Marcus J. Ranum about her early interest in computers and the path that lead her to become head of IT and compliance for the company's global business units.

MARCUS RANUM: Was there anything you'd identify in your childhood that set you on a course for your professional career? How did you wind up where you are now?

DYANN BRADBURY: Where I was raised, you grew up, went to high school, got married, had a job—only you were a farmer's wife—and that's it. Or you were a secretary or taught school. I happened to get a job at a bank when I was in high school, so I could go there and work in the morning for a couple of hours. I think it was 1979, and I graduated from high school in 1980 and was scheduled to be married in 1981.

I went in to the senior vice president of the bank and said, 'I want to take some [college] classes; what do you suggest?' And he said, 'Why not learn about computers because everyone is going to have one on their desk in 10 years.' I took 'Intro to Computers and Data Processing' and got so interested in it that I decided I needed to know everything there is to know about computers—everything

from how the current comes in to the power supply, to how the software works. What sparked my passion was how the computer read the information—yes/no, on/off. I thought, this is incredible!

By then, I was working full time, I was married, and I was taking night classes. I took electronics classes—transistors and base-level stuff, [including] computer repair. They would give us a motherboard and [computer] case, a drive [and say,] 'make it work.' I took classes in networking from beginning to advanced.

So this was all early '80s—probably a Z80 [Zilog 8-bit microprocessor] or an 8088-based CPU board. Neat!

I learned how to solder, populate a board with chips. I remember the advanced networking lab: The lab tech took out segments of cable and replaced some of them with bad cable; he removed the jumpers from network cards and threw them in the middle of the room, that sort of stuff. We had to build boot floppies that would get the system up and running after diagnosing and fixing all the flaws in the network. Anyway, I passed it and *loved* it. I did very, very well.

Then it was time to upgrade the bank's data processing systems, and I contacted the data processing center and said, 'Just send me the equipment, and I'll upgrade it.' Well, I did that and they offered me a job. So I came to Lincoln, [Neb.]—and by then we had our son—and applied for an engineering position. And everything needed

Dyann Bradbury

to be upgraded well in advance of Y2K. We were told that failure was not an option. We had a project to convert 250 banks from Novell [Netware] to [Windows] NT in 18 months. There were 13 of us. We averaged three hours a night of sleep; we were on the road one week installing systems then back the next preparing for the next install. I was configuring [Microsoft] Exchange servers, SQL servers, converting Novell to NT, running and terminating cable, the whole thing. We'd walk into a bank at 3:00 p.m. in the afternoon, and we had to have everything up and running and converted by 8 a.m. the next day. We all shared the responsibility and the opportunity.

That's really hardcore.

I was thrown into the fire and I learned so much. And I was the only woman. I went from an engineer all the way to a senior engineer. Bam, bam, bam!

When did you start getting into security?

I've never had a position that has had *security* in the title. It's always been *engineer* or *analyst* or *compliance*. I've been mostly a manager. Security should be part of *all* IT, no matter if you're putting in a firewall or configuring a desktop or a server.

We're a side effect of bad systems and network administration.

But I do consider myself a security person because, in everything I do, it's a consideration. Right now, I oversee global compliance. So if a business is thinking of developing a new system that touches customer card data, they'll call me into the meeting—anything from an IT and compliance perspective, I consider that security. Anything from a product offering to setting up a new data center to developing new code—it's all security. I get called into the room when they're setting up anything that affects the business.

That's one of the things I keep yelling about: This is all something that has to be embedded in! It's all part of system reliability. You wouldn't build a new data center that didn't have uninterrupted power supplies or redundant network links, would you? Security is an operational consideration; it's *part* of building reliable systems.

Our job is making the business realize that this stuff is important, and if we don't approach it this way, we're making false economies. You have to ask the right questions. You have to understand the business—the data, the services you're offering, what products are in use. You have to have a full understanding of the *entire* infrastructure … because when you introduce something, it affects everything.

Engineering at its highest [level] is understanding interactions between loosely coupled, connected processes.

It's also the controls that you have in place for all of them. You introduce something in here; it's going to change that. How do we need to change the controls? So you need someone that understands it from a reliability, security, global compliance and legal perspective. That's why [you should] always approach things so that there's no division. We're all working toward a common goal. You cannot have division between compliance and security.

I don't see many organizations that do that. Thanks to some standards like [those for the] Payment Card Industry, Sarbanes-Oxley and the HITECH Act, I think we've created separate priesthoods that see compliance as a goal in its own right.

We've had to start going through audits, and building an IT and compliance program was one of my first responsibilities. My role is to build that trust between IT and compliance—my technical background helped there. I can tell in a few minutes if someone's trying to BS me, and it doesn't work. And I know what it takes for someone to do their job because I've done it and I respect their work. I also serve as a liaison between auditors and IT, and I can start pulling people out if they start going down a rabbit hole. I can advocate [for] either side and be a buffer between them.

Computer security is a boy's club. As much as I hate to ask, has being a woman ever been a problem for you?
Sure! I remember one time when I was a junior system engineer and the lead systems engineer said, 'I give her two weeks.' I stuck it out, and I was promoted, and he always asked me to work with him in the future. The boy's club mindset breaks down as you move up the management tree. Organizations know you can't afford that sort of behavior as you get more senior; it wastes energy.

Sometimes you have to prove yourself immediately—but in a respectful and productive way. As leaders, we have to look at how our people treat other people; it's part of mentoring. ■

MARCUS J. RANUM, *the chief of security at Tenable Network Security Inc., is a world-renowned expert on security system design and implementation. He is the inventor of the first commercial bastion host firewall.*

TechTarget Security Media Group

TechTarget
275 Grove Street,
Newton, MA 02466
www.techtarget.com

COVER IMAGE: GRANDFAILURE/ISTOCK