Companies Aren’t the Only Ones Migrating to Cloud

Data protection is harder as threat actors embrace all the advantages of cloud. Here’s what to watch out for in 2018.
Breaching the Tipping Point

While the EU is taking steps to protect residents’ data, little has happened in the United States.

EQUIFAX ADMITTED DURING its Q4 2017 earnings call in March that more people, than previously disclosed, had their personally identifiable information—names and partial drivers’ license information—exposed in the company’s historic data breach. And there may be more, the consumer credit company told regulators. With 147.9 million consumers affected, and counting, what will the data privacy breach cost Equifax?

That same month, Facebook came under fire for mis-handling the data privacy of 50 million users. Roughly 270,000 Facebook users had downloaded a psychology professor’s app, and their data and that of their “friends” was allegedly harvested in 2016 by political data firm, Cambridge Analytica.

Unlike Americans, citizens and residents of the European Union will soon have strengthened data privacy breach protection when the EU’s General Data Protection Regulation (GDPR) goes into effect on May 25, 2018. Instead of a credit freeze and lifetime of credit monitoring, individuals in the European Union can look to data authorities to enforce 72-hour breach notifications and impose hefty fines for data privacy breaches.

Whose data will the GDPR requirements protect? The data of residents—regardless of their nationality—of the European Union’s 28 member states. “They can be in transit, cross border [or in the United States] on tourist activities. As long the person resides in those 28 states, the regulation applies,” said Michelle Robles, principal consultant at Dimension Data.

Robles said she advises companies to focus on data principles that apply to the privacy-by-design requirements of Article 25, data protection by design and by default, which “hits at the heart of GDPR.” Article 25 requires organizations to implement mechanisms to protect data subjects’ rights—security is just one of those controls. “Most organizations in America have had a lot of challenges around consent and privacy by design,” Robles said.

If the data subject wants their data forgotten or transported, the organization has to comply and provide transparency into that process, essentially an audit trail. How do companies electronically transfer that information, and where does their responsibility to the data subject end? Organizations struggle with those challenges and...
more as they begin to address the 99 articles outlined in the GDPR requirements.

The retail and tourism industries have been proactive with their GDPR requirements, according to Robles. “They understand the gravity of it, and they have hired companies to help them with the complexities.” Smaller and midsize organizations are struggling with the interpretation and overall effort it takes to meet the GDPR’s objectives because it’s so expansive. The 72-hour data privacy breach notification of data authorities is another hurdle that may require “heavy lifting” to avoid insurmountable data breach cost. Companies need to work on their breach notification process and test it periodically.

While the EU is taking major steps to protect residents from a data privacy breach, little has happened in the United States. When the Equifax breach was revealed, many people thought it was a tipping point. Surely, the credit ratings company’s exposure of millions of consumers’ personally identifiable information would spark legislation and criminal proceedings that would serve as a warning to other companies. That hasn’t happened.

In March, Equifax beat analysts’ Q4 2017 profit expectations. Costs associated with the “cybersecurity incident” for the year totaled $164 million, with $50 million offset by insurance. A few days before the earnings call, Equifax hired “permanent” CISO Jamil Farshchi, who previously worked at Home Depot, Time Warner, Visa and NASA to replace interim CISO Russ Ayres. Company officials project $275 million in gross costs associated with the cybersecurity incident in 2018, offset by $75 million in insurance. Facebook may pay a steeper price.

KATHLEEN RICHARDS is the features editor of Information Security magazine. Follow her on Twitter: @RichardsKath.
When Apple Inc. launched its iCloud service in 2011, cloud threats didn’t include the Chinese government. Apple changed its policy in February of this year and conceded to Chinese authorities’ demands to store mainland residents’ encryption keys in data centers in the People’s Republic of China. Housed on local servers, run by state-backed Guizhou-Cloud Big Data Industry Co. Ltd, experts fear the Chinese government could gain access to users’ private data. Apple may be one of the wealthiest company’s in the world, but even it cannot guarantee data security in the cloud.

Consistent security for all data from third-party partners and cloud providers is what many consider the next evolution of cloud. Even when the risks associated with cloud threats are high, the cost benefits—in Apple’s case, access to a market with the world’s largest purchasing power—outweigh the risks. This matters more and more as use of cloud services grows.

Enterprise spending for public cloud services worldwide is expected to reach $160 billion in 2018, according to International Data Corporation, up 23.2% from 2017. In the U.S., discrete manufacturing, professional services and banking industries are forecast to spend the most this year on public cloud services.
Software as a service continues to have the highest growth as Microsoft, Oracle and SAP migrate their on-premises enterprise customers to subscription services in the cloud. Spending on infrastructure as a service—AWS, Microsoft Azure and others—is next, followed by platform as a service (PaaS) offered by Amazon, Microsoft, Salesforce, Google App Engine, Heroku Enterprise and more. Companies are using PaaS—operating systems and hardware—for rapid development, testing, deployment and increasingly, data management.

MORE POWER IN THE CLOUD
Most platforms take advantage of public cloud security features, but large-scale clouds don’t always mean large-scale threat protection. What cloud threats should you watch out for in 2018?

Malicious cryptomining is one of the leading types of attacks since September 2017, according to Malwarebytes Labs. With the volatility in the Bitcoin market—described as the next gold rush—it’s no surprise that hackers who need massive processing power to verify and confirm transactions to blockchain have found their way to cloud servers in an attempt to earn more digital currency.

In February, hackers accessed an Amazon public cloud account, owned by electric carmaker Tesla, using credentials obtained through an unsecured administrative console in Kubernetes open source orchestration software. The Tesla breach had similarities to cryptocurrency mining malware detected in the Amazon and Microsoft public clouds of SIM card manufacturer Gemalto, and multinational insurance provider Aviva, according to RedLock, the cybersecurity startup that disclosed the attacks. But the Tesla hackers used different techniques to cover their tracks. Instead of using a public mining pool—groups of cooperative miners, largely based in China—they installed “mining pool” software, hid the IP
address of the server behind Cloudflare and configured the software to a nonstandard port, according to security researchers. The attackers also accessed sensitive telemetry data and other nonpublic information Tesla stored in an Amazon Simple Storage Service (S3) bucket. Tesla addressed the security problems when RedLock notified the car company.

A Los Angeles Times website called The Homicide Report maps murders and homicides—633 people were killed in the last 12 months—in LA County. In February, attackers discovered an unsecured AWS S3 bucket. They embedded the popular cryptojacking malware Coinhive into the website for drive-by mining of visitors’ browsers and PCs. Security researcher Troy Mursch discovered the embedded JavaScript, used specifically to mine Monero, an open-source cryptocurrency released in April 2014. Author of the Bad Packets Report blog, Mursch’s internet research tracks cryptojacking and internet of things (IoT) botnets.

Linux malware that attacks embedded systems to build botnets—similar to Rakos—is going to become more prevalent. “The reason we haven’t seen it in the past is because, by trade, the people who are writing malware and doing these intrusions are heavily Windows-based,” said Mounir Hahad, head of threat research at Juniper Networks Inc. in Sunnyvale, Calif. “But as it turns out, it seems like there’s a lot of money to be made in cryptocurrency, and it is so much easier to attack IoTs with Linux malware.” In December, Juniper Threat Labs discovered Linux malware on a popular home brand of DSL routers used to build an IoT botnet for cryptocurrency mining. Juniper notified the manufacturer. Hahad expects to see more IoT botnets used for Bitcoin mining because many IoT embedded systems are Linux-based.

SIGNING UP BOTNETS

Data shows a rise in the number of attackers that consume public cloud services to host command-and-control servers for IoT botnets and ransomware. In January, the Spamhaus Project, a nonprofit based in Geneva, released its 2017 Botnet Threat Report. Researchers at Spamhaus Malware Labs identified more than 9,500 botnet command-and-control servers on 1,122 different networks. Botnet controllers, according to Spamhaus’ block listings, increased 32% in 2017, and that data does not include controllers hosted on the dark web, where servers can’t be identified. “What stands out in 2017 is the dramatic increase of botnet controllers hosted at cloud providers,” the researchers stated. Large botnet operators are cloud threats, deploying botnet controllers in public clouds.
such as Amazon Web Services and Google Cloud Platform (Compute Engine) using fraudulent signups. “While some of the cloud providers managed to deal with the increase of fraudulent signups, others are obviously still struggling with the problem,” researchers said.

Botnets increasingly pose a number of types of cloud threats, powering distributed denial-of-service, ransomware and other crippling attacks. Ransomware remains one of the most lucrative for cybercriminals, who can easily find ransomware kits online; more than 4,000 online sites sell roughly 45,000 ransomware products and services, according to McAfee’s February report “The Economic Impact of Cybercrime.”

While ransomware is on the radar of most companies and law enforcement, threat researchers like Hahad expect to see an uptick in ransomware as a service. “I think we are going to have deal with that threat very seriously,” he said. “We’re getting a lot of relatively low-level, low-skilled cybercriminals taking advantage of other people who want to stay hidden and who have the capabilities to develop some pretty potent malware.”

Some of these issues are enterprise problems, but some are not. In the shared-responsibility model for public cloud security, cloud providers secure the physical data centers and protect their network systems against attacks. Companies consuming cloud services are responsible for the rest: configuring and launching cloud instances, managing identity and access controls, updating security controls to match configuration changes, and most importantly, protecting workloads and data.

The architectural flaws in Intel and Advanced Micro Devices chip designs, like the Meltdown and Spectre vulnerabilities disclosed by security researchers in January, fall into the realm of cloud providers, however. The vulnerabilities require updating the CPU’s firmware microcode and operating system. (Intel reportedly warned its Chinese technology customers about the critical security flaws before it divulged them to the United States government.)

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

WHAT CISOs EXPECT IN 2018. —Kathleen Richards

What do you predict will happen to your organization in 2018?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Threat Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>65%</td>
<td>Phishing scam that results in credential theft</td>
</tr>
<tr>
<td>61%</td>
<td>Disruption to processes caused by malware</td>
</tr>
<tr>
<td>59%</td>
<td>Cyberattack that causes significant downtime</td>
</tr>
<tr>
<td>53%</td>
<td>Data breach involving 10,000+ records</td>
</tr>
<tr>
<td>50%</td>
<td>Leakage of confidential information/emails</td>
</tr>
<tr>
<td>44%</td>
<td>Third-party misuses or shares confidential info</td>
</tr>
<tr>
<td>31%</td>
<td>Economic espionage</td>
</tr>
<tr>
<td>25%</td>
<td>Cyberextortion, such as ransomware</td>
</tr>
<tr>
<td>21%</td>
<td>Nation-state attack</td>
</tr>
<tr>
<td>18%</td>
<td>Noncompliance fine</td>
</tr>
<tr>
<td>14%</td>
<td>Attack against IT structure, resulting in damage</td>
</tr>
</tbody>
</table>

Which of the following threats do you worry most about in 2018?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Threat Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>70%</td>
<td>Lack of competent in-house staff</td>
</tr>
<tr>
<td>66%</td>
<td>Data breach</td>
</tr>
<tr>
<td>59%</td>
<td>Cyberattack</td>
</tr>
<tr>
<td>54%</td>
<td>Inability to reduce employee negligence</td>
</tr>
<tr>
<td>48%</td>
<td>Ransomware</td>
</tr>
<tr>
<td>47%</td>
<td>Breach due to IoT devices in the workplace</td>
</tr>
<tr>
<td>42%</td>
<td>Third-party data breach</td>
</tr>
<tr>
<td>34%</td>
<td>Inadequate budget</td>
</tr>
<tr>
<td>25%</td>
<td>Inability to reduce insider risk</td>
</tr>
<tr>
<td>25%</td>
<td>Compliance failure</td>
</tr>
<tr>
<td>19%</td>
<td>Nation-state attack</td>
</tr>
</tbody>
</table>

MULTIPLE RESPONSES PERMITTED

SOURCE: “WHAT CISOS ARE WORRIED ABOUT IN 2018,” JANUARY 2018, PONEMON INSTITUTE; N=564 CISOS AND INFOSEC PROFESSIONALS; ART: PENFOLD/GETTY IMAGES
Is your company likely to have a data breach or cyberattack in 2018?

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate in-house expertise</td>
<td>65%</td>
</tr>
<tr>
<td>Inability to protect sensitive and confidential information from unauthorized access</td>
<td>59%</td>
</tr>
<tr>
<td>Inability to keep up with the stealth and sophistication of the attacker</td>
<td>56%</td>
</tr>
<tr>
<td>Failure to control third parties' use of our sensitive data</td>
<td>51%</td>
</tr>
<tr>
<td>Unable to replace legacy systems and technologies</td>
<td>45%</td>
</tr>
<tr>
<td>Not enough employee training to prevent negligent behavior (phishing/sharing passwords)</td>
<td>36%</td>
</tr>
<tr>
<td>Inadequate budget</td>
<td>33%</td>
</tr>
<tr>
<td>Inability to control the proliferation of IoT devices in the workplace</td>
<td>30%</td>
</tr>
</tbody>
</table>

If yes, why?

What do you predict will happen to your career in 2018?

<table>
<thead>
<tr>
<th>Prediction</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job will become more stressful</td>
<td>69%</td>
</tr>
<tr>
<td>Lateral move within company, not in IT security</td>
<td>44%</td>
</tr>
<tr>
<td>Completely change careers</td>
<td>41%</td>
</tr>
<tr>
<td>Join another company, not in IT security</td>
<td>36%</td>
</tr>
<tr>
<td>Receive a promotion</td>
<td>27%</td>
</tr>
<tr>
<td>Terminated or demoted</td>
<td>23%</td>
</tr>
<tr>
<td>Higher salary</td>
<td>17%</td>
</tr>
<tr>
<td>Join another company, in IT security</td>
<td>16%</td>
</tr>
<tr>
<td>Retire</td>
<td>11%</td>
</tr>
<tr>
<td>Job will become less stressful</td>
<td>9%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

MULTIPLE RESPONSES PERMITTED

Source: “WHAT CISO'S ARE WORRIED ABOUT IN 2018,” JANUARY 2018, PONEMON INSTITUTE; N=564 CISOs AND INFOSEC PROFESSIONALS; ART: QVASIMODO/GETTY IMAGES
AMAZON WEB SERVICES takes unusual measures to prevent data from leaving its data centers, estimated to house between 50,000 to 80,000 servers. Physical hard drives are shredded, hole-punched, totally destroyed. Google follows a similar practice.

“Humans and data don’t mix,” said Stephen Schmidt, the CISO for AWS, during the company’s Security State of the Union summit last November. “Keep the people away from the data.”

While those tactics may sound extreme to many companies, human error has taken its toll, leading to high-profile data leaks in the cloud, chiefly with AWS S3 security. Instead of developers using Amazon’s internet cloud storage, untrained IT staff and business personnel are depositing data in the cloud.

“We tend to think about misconfigurations and AWS buckets as being something a very skilled IT professional has done, when no, that’s not the case,” said Mounir Hahad, head of threat research at Juniper Networks Inc. in Sunnyvale, Calif. “Very often, a group that has no relationship with security went ahead and created something because it was an easier and faster way to transfer data. The next thing you know, the whole network is open to the world, and the data is leaked.”
Financial publisher Dow Jones & Co., owned by News Corp., confirmed reports in July 2017 that the company may have publicly exposed personal and financial information of 2.2 million customers, including subscribers to The Wall Street Journal and Barron’s. The leak was traced back to a configuration error in a repository in AWS S3 security. Dow Jones had intended to provide “semi-public access” to select customers over the internet. However, access to download the data via a URL was granted to “authenticated users,” which unfortunately included anyone who registered (for free) for an AWS account.

**BIG-NAME PROBLEMS**

Accenture, Verizon, Viacom, Tesla and Uber Technologies are just some of the high-profile names in the steady stream of companies that have exposed sensitive information via AWS S3 security misconfigurations. Some users forget to set up AWS bucket password protection; others don’t understand basic features in Amazon such as resource-based access policies (access control lists) or bucket permissions checks and unwittingly expose data to the public internet.

Customers have their choice of security configurations in the cloud, but Amazon is also taking steps to help IT security teams enforce behavior through tooling.

In November, the company updated its AWS dashboard, encasing public in bright orange on the AWS S3 console so that cloud customers could easily see the status of access permissions to buckets and their objects. “We want to make it super obvious when your S3 bucket is open to the

---

**One-Year Plan: Amazon’s ‘Mechanisms to Drive Security’**

AWS CISO Stephen Schmidt works with his team to set a series of expectations for the year. And there are measurable service goals for every service team in the company. A major aim is to “radically restrict” human access to data, which means restrict it by 80%, according to Schmidt. “It’s to drive people to use tools for things that they would otherwise do by hand.”

Schmidt’s one-year plan includes the following:

- buy-in from leadership;
- radically restrict and monitor human access to data;
- source code security;
- patching;
- log retention duration;
- credential blast radius reduction;
- credential lifespan reduction;
- Transport Layer Security implementation;
- AWS encryption everywhere; and
- canaries and invariants for security functionality.
public,” Schmidt said.

The company added default encryption to all objects when they are stored in an AWS bucket and access control lists for cross-region replication. This functionality is free. Another new tool—codenamed Zelkova—is aimed at AWS S3 security policies to help users identify which one is more permissive than the others. Amazon Macie, a managed service that uses machine learning to detect personally identifiable information and intellectual property, has been available for S3 since August. It works with CloudTrail, Amazon’s log management service. According to Schmidt, every new service or feature—1,042 in 2017 alone, as of the end of November—has to go through a security review. Almost half of the AWS functionality introduced in 2017—467 features—focused on security.

As with on-premises networks, information security in the cloud requires continuous monitoring: How often are people logging into systems? Does the IT staff check who is accessing source code?

“When you go to the cloud, you are actually facing a new reality,” Juniper Networks’ Hahad said. “Unfortunately, there is a misconception among a lot of IT organizations that whatever happens in the cloud is kind of not their responsibility.

“I think IT organizations all the way up to the CISO should not abdicate their role—they are the guardians of any intellectual property. What we see happening very often is that they allow various entities within the organization to go ahead and create AWS or Microsoft accounts, and you lose control over what is going on.”

Amazon’s own model is driven by security expectations and leaves little to chance. The company keeps careful constraints around its staff, watches what they do every day and instructs service teams to restrict access to data through tooling and automation. In addition to privilege separation, Amazon rotates credentials and enforces short lifespans—sometimes measured in hours, according to Schmidt.

STILL NOT PATCHING
The biggest threats to cloud data for most companies involve misconfiguration or lack of patching, noted Andrew Nielsen, formerly CISO at Druva, a data management-as-a-service startup based in Sunnyvale, Calif. “So many organizations have been breached because they didn’t keep up with patches,” Nielsen said.

Cloud data management services are on track for growth, attracting startups such as Druva and Rubrik as more companies look for data center backup and recovery. Emerging companies are entering a space dominated by Dell EMC, IBM, Commvault, Veritas Technologies and others.

“The struggle we see is a lot of organizations are really good at managing infrastructure in their data center—they’re maturing their tooling, and they’ve got operational procedures—but when they move to cloud, a lot of that shifts,” Nielsen said. “They need new tool sets along with skill sets that they’ve got to acquire, and that’s where we see a big gap.”

What’s the best way to deal with patching? “Shoot the old version in the head once you have the new one run-
“Amazon can show you there was a network connection, but what they can’t do is show you what is happening inside the operating system or the server.”

SAM BISBEE, Threat Stack

How can CISOs better manage configuration changes? With the shift toward DevOps, new intrusion detection platforms—such as Threat Stack—look at malware and remote adversaries breaching environments and what internal employees are doing in production. The subscription-based software as a service integrates with products—DevOps tools (like Chef and Puppet), Amazon machine instances, Docker and more—that IT teams use to configure and automate their deployments. The technology supports cloud configuration auditing, behavioral analysis and threat detection across hybrid cloud infrastructures.

Other companies in the AWS cloud security and compliance space include CloudPassage, Dome9 Security and Evident.io.

“Amazon can show you there was a network connection, but what they can’t do is show you what is happening inside the operating system or the server,” said Sam Bisbee, CSO at Threat Stack, a Boston-based startup.

“When Alice logs into the production database, what does Alice actually do when she logs in? Are engineers leveraging all [of our] build pipelines and this great automation? Or are they logging into servers and manually changing config files, which creates availability, security and compliance concerns,” Bisbee said.

Greater visibility may help as problems with AWS S3 security continue to plague companies, both large and small. Putting a stop to AWS bucket misconfigurations may require enacting policies that limit the damage caused by untrained or careless employees.

“It is kind of hard to say [this], but I personally believe that sometimes you have to implement heavy penalties for infractions,” Hahad asserted. “The CISO should tell employees of the company, ‘Here is the framework within which we are going to work, and any division from this framework is going to be penalized.’”

Make people accountable, he advised, “and you will have a lot of ammunition to hold that position.”

KATHLEEN RICHARDS is the features editor of Information Security magazine. Follow her on Twitter: @RichardsKath.
Tech Checkup With Health CISO
Joey Johnson
Cybersecurity and healthcare can get along, according to Johnson, but it takes attention to the details.

PRESIEME HEALTH MANAGES more than 500 employer-sponsored health and wellness centers, including many at Fortune 1000 companies. As the concept of on-site clinics, pharmacies, wellness seminars and employee health flourishes, the healthcare provider based in Brentwood, Tenn., has grown to 4,500 employees. In the CISO position at Premise Health since 2010, Joey Johnson has witnessed a sea change in security, especially in the last five years. “Cybersecurity has now become more front and center,” he says. The security veteran has weathered the business transformation: He was named 2017 CISO of the Year by the Nashville Technology Council.

Johnson held the CISO position for CHS Health Services, which merged with Take Care Employer Solutions to form Premise Health. Before becoming a healthcare CISO, he served as the CSO for the United States Department of Commerce, Office of Computer Services. An outspoken security evangelist, Johnson is on the technical advisory board of Landmark Ventures and the editorial board of the Journal of Law and Cyber Warfare. In this Q&A, the healthcare CISO speaks about the growing challenges of information security and privacy in the healthcare industry.

What is your infrastructure like, and how does it reflect your company's approach to healthcare delivery?
As a healthcare company, we are a little unique because we provide on-site wellness to large, self-insured companies, typically global financial and technology institutions. Most are Fortune 100 or Fortune 500. For those organizations, we are the gateway to broader use of the healthcare ecosystem. We handle eligibility files, birthdates and Social Security numbers on an entire workforce. So, obviously, between those kinds of demographics and actual patient data, that is a lot of sensitive information that our clients care about, and that has resulted in intense scrutiny on us. We are constantly being audited. We have a security operations team and [an] in-house ISAC [Information Sharing and Analysis Center] that run all kinds of things. They are always looking for problematic things and making sure we
We have a dedicated penetration testing team. They pick at applications and try to make sure we are proactive. There is a governance, risk [and] compliance team for policies and procedures, risk mitigation and conducting incident response. Like most organizations, we also have identity access management functions that sprawl across all parts of the environment. And we have a large third-party risk management function. They are the liaison to the rest of the business. They engage with legal, privacy, compliance, HR, finance and all the business units. All of these roll up to me. In the CISO position, I have a broader, more strategic role as I engage with the rest of the C-suite.

You can’t protect everything. As a former national security adviser said, ‘If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds,’ [attributed to McGeorge Bundy, national security adviser to President Johnson and special assistant to President Kennedy]. You must understand what normal activities are and what your crown jewels are—and that takes a lot of time, effort and tuning.

**What is the biggest cybersecurity challenge for a healthcare CISO?**

I think the biggest challenges I face aren’t necessarily unique to healthcare. One is the **skills shortage**. Another I face is the strategic decisions you make on which technology to bring in and support. Obviously, ‘there’s gold in them hills’ as far as security products. But there’s a lot of noise, too, and we have to investigate. I will often see other organizations with overlapping solutions—products that were brought in and didn’t get optimized and then **new tools** were brought in that overlap. So they are just throwing money at a problem. The biggest challenge at most organizations is that it is still security functionality 101. You need to let the data in your organization tell you what is going on and then build an appropriate security model around that. It is like going to the gym. It is not...
easy. It takes patience and determination. Then, if you do it right, product selection becomes clearer.

If you are hearing you need threat intelligence feeds, maybe you do. But if you don’t have a good grasp on log file correlation and you have SIEM and it is working well, maybe you aren’t at that place where you can really understand your own traffic. In that case, all that threat intelligence feeds will tell you is there is a tornado coming. But if you don’t know the problems you have today, you are not going to be able to digest that extra information. Many organizations are struggling with this [issue]. Orchestration solutions are coming. That’s great if you are ready to use them but not if you haven’t optimized the solutions you have.

Furthermore, once you begin something, you have to have the resources to stand it up and manage it. Do your hygiene and patching, and that will take you a long way. It isn’t a sexy answer, but those are the critical things an organization needs to focus on. While the threat landscape changes, your assets don’t change that often.

**Are you able to sufficiently encourage safe cyber practices across a geographically and professionally diverse workforce?**

How do you convince a doctor that protecting data is as important as preventing an infection or making a correct diagnosis? Absolutely, it is a battle. It is a battle in any organization. Doctors, who took the Hippocratic Oath, want to protect patient safety and well-being, but part of that is protecting their privacy. I think they understand that. The frustration comes in understanding how the security controls are aligned to their world. Our workforce knows the companies we serve are concerned about this. But with that said, things like phishing are still a threat. With 600 sites, the best you can do is to try to get close to the workforce and have a consistent message that resonates.

**As a healthcare CISO, are you using or preparing for things like ‘telemedicine,’ where doctors consult remotely?**

Telemedicine is one direction. I think pretty consistently we are always preparing a plan for where we are going. Technology is a big part of our organization. It is sort of expected when you are delivering healthcare services to software companies, computer hardware companies and manufacturing companies in general. The bar is very high on what they will accept from a technology perspective. They are pushing the envelope. They want it to be innovative and high functioning. Part of the challenge from a business perspective is that we are balancing where our clients want us to go versus where we think we want to go. On the back end, we need to make sure as we go and explore new frontiers that we are also taking security into consideration. We are often going down paths where best practices haven’t been established yet.

**As your company expands, does the CISO position have input into how? In other words, is the voice of cybersecurity also heard?**

I think, particularly as a healthcare CISO, I am of the perspective, and I know my organization is, that security is not what it was even five years ago. I have been doing
this for 20 years, and cybersecurity has now become more front and center. However, to be effective, you need to understand the business on the terms of the business. Ironically, while you are serving as security lead, you must take off your blinders and understand business—where the puck is headed—and be able to implement the things that feel like a win for the business.

If you are fighting to make everything as secure as possible, you can lose your audience. On the flip side, business needs to understand how to interact with the security function. With the solutions out there—whether that is Dropbox or collaborative platforms—if you don’t make it easy for the workforce, they will find a way around it. It isn’t like 20 years ago when you were the only source of access to computer power. Data moves. If you don’t make it easy to do it securely, they will find a way around, and you will end up swimming upstream.

ALAN R. EARLS is a Boston-based freelance writer focused on business and technology.
The Many Hats of Joe Grand

Computer hardware designs with dangerous security flaws? That’s no surprise to renowned hacker Grand.

SECURITY RESEARCHER JOE Grand focused on hardware vulnerabilities long before Spectre and Meltdown made headlines. An electronics guru who co-hosted the popular Prototype This! TV series on the Discovery Channel, Grand has educated people about hardware hacking since his teens. Known as Kingpin, Grand was part of the hacker collective L0pht—named after the group’s loft in Boston’s South End. The underground security researchers tested the limits of technology and cyberspace, and promoted responsible disclosure. The group, including Grand, warned a Senate Governmental Affairs Committee in 1998 that hardware and software linked by networks and the internet posed a serious security threat that was hard to solve and would only get worse.

The members of L0pht joined with venture capitalists to form @stake, a security firm that was acquired by Symantec in 2004. Along the way, Grand earned a bachelor of science in electrical engineering from Boston University. Since 2005, Grand has taught a two-day course at Black Hat: Hands-on Hardware Hacking. The annual training course is focused on reverse engineering and “defeating the security” of embedded systems and devices. He is also the engineer who designed DEFCON’s hackable circuit-board badges, first used in 2008. In addition to his work as an engineer and hacker, Grand is an inventor and founder of Grand Idea Studio. Here, Grand discusses hardware vulnerabilities in the wake of Intel’s flawed chip designs, and the ramifications for mobile devices and the internet of things (IoT).

The Spectre and Meltdown bugs turned out to be a huge problem for complex CPUs, and the software side of the world is struggling to fix hardware vulnerabilities. Should we expect to see comparable problems with less-powerful hardware like IoT devices or phones?

Those are highly complex architectural design flaws, and I think we’ve only seen the beginning of those types of attacks—things that jump through many hoops to get something done. We’re seeing them on servers and systems, where it’s easier to focus because they’re powerful. But we’re going to see those types of attacks move down the hardware spectrum, sort of a trickle down to less-capable
devices. There are going to be some that are specific to specific architectures.

The real problem is that we don’t even need such complex attacks for most of the internet-connected devices. ... There are so many other ways you can get in.

**Should we assume that mobile phones are suffering the same sort of problems and they just haven’t been explored yet?**

Mobile phones are highly complex, not as complex as a desktop or server but much more complex than an IoT device. We’re going to start seeing more of these potentially damaging design-flaw exploits that result from subtle interactions in the hardware.

I saw a demo at the CanSecWest Applied Security Conference back in the early 2000s where someone exploited a buffer overrun in a smart antenna controller chip in a cellphone, then created a running UID=0 process [unique ID superuser privileges] in the Linux kernel. I walked out of there thinking, ‘We are so screwed.’

Yes, and the thing is that there are so many subsystems in devices now. In the rare instance that you have a hardened system, you’re going to have some peripheral, or some module, or something that could be vulnerable, and it’s all connected. Another great example is a hack that was demonstrated at Chaos Communications Congress, where Hunz [the hacker] was hacking an Amazon Dash and found a way of compromising the device using a hole in the audio processing function. He could execute arbitrary code by sending sounds at the device. There are other examples of game consoles, which tend to be some of the most secure consumer devices out there because so many people hack on those; attacks can work against peripherals for the device—attack the controller or a USB audio device. It just takes one vulnerability in one thing, and it’s very hard to anticipate where everyone is going to attack.

There was an incident where someone figured out a way around digital rights management by exploiting a bug in a graphics card driver. The driver was signed by the manufacturer, so Windows would cheerfully load it into kernel space. The attack would take over the driver, and presto! the entire system memory was available for capture, including digital rights management keys and data.

I think it’s going to get worse. What I see happening a lot is people who are not traditionally hardware hackers starting to get into embedded system hacking because the barrier to entry for getting involved has gotten much lower. Every device that’s connected to a network is a computer now. You don’t need to be a hardware engineer to exploit these devices anymore—you can be an operating system-level hacker because there’s an operating system in there too.

There is a continued lack of security understanding by engineers, and because so many products are becoming connected, people are slapping in network connectivity, which makes it vulnerable. But you can’t blame engineers because it’s a completely different and very challenging field. All these things combine to continue to make it happen even more.
As a systems administrator, I look at the same scenario you’re describing: All these devices are going to be running some operating system, and people are going to just assume they don’t need to worry about software reliability or operating system flaws.

That’s exactly right. People take a piece of hardware and take it for granted because it’s in a nice box; it has some LEDs. Connect it to the network, plug it in, and it’s up. A lot of these devices don’t have any sort of patching capability or firmware update capability, and if they do, it’s probably insecure. That opens up a whole other world of attacks. It ends up being a system administration issue that is very hard to deal with because there are so many entry points into the platform.

I remember last year when I said, ‘Hardware is the stuff you run software on.’ You looked at me and said, ‘It’s all software.’

The hardware, if it’s not a PC or a server, has a slightly different set of entry points above and beyond what you would with a network-connected type of thing. If you have physical access to a hardware device, you can possibly get access to debug interfaces like JTAG, [an Institute of Electrical and Electronics Engineers communications standard named after the Joint Test Action Group and used to test circuit boards], which would then give you direct access to memory. You’ve got access to console output, backdoors and reset codes—all of those are entry points into the hardware electronics, but the real goal is to get access to software. Then it becomes a software problem.

And, on top of all that, some software engineer is going to leave a debugging backdoor in the software layer, for their convenience, and they forget to turn that off in production.
Or it might be intentional because then that way, if they have to reset a device for a customer, they have an entry point. A lot of vendors leave that in for convenience purposes—it’s the ‘security versus convenience’ problem we’ve talked about for decades, and convenience usually wins. But it’s also that developers are not necessarily thinking, ‘I’m going to leave that backdoor in and someone is going to use it for malicious purposes.’ They leave it in for their purposes and aren’t trained to think about what happens if someone else uses it as well.

**For me, finding out about the Intel Management Engine (IME) was a heart-stopping moment of terror. I still wonder if someone thought that up and said, ‘This is a good idea,’ or if the NSA helped encourage that mistake.**

The complexity of that, and the complexity of CPUs, that’s where this stuff hides. It’s a CPU inside a CPU, and it’s running Minix in there. Probably nobody in the world except a few people knew or cared that was in there. It’s mind-blowing that you have these layers of computing functionality even within a single device—the IME, Spectre, Meltdown—those things mean we’re going to have to keep trying to educate people about security and risk. It’s terrifying. Being security researchers, we’re supposed to be at the state of the art, and these kinds of things keep getting dropped—it’s phenomenal!

You’re working with all these new microprocessors that are highly integrated—that have all kinds of capabilities, like complete TCP/IP stacks, waiting to be invoked. I heard someone talking about using a component that had an IP stack. They didn’t need an IP stack, so they were just going to leave it there. What could possibly go wrong? It sounds like [hardware vulnerabilities] are going to be a gift for the hackers that keeps on giving.

I think it might come down to education. That’s something I teach people in my hardware hacking class: Nothing is secure, but you can choose the right sort of thing. If you think about software development, people will write what they need and will make mistakes, but software can be patched. With hardware vulnerabilities, the bugs are baked into physical silicon and it can’t be changed. I don’t think the hardware developers are malicious; they’re just working in a medium that doesn’t change. If you have a bug or a ‘feature’ like IME in your hardware, you’re completely screwed if it can’t be turned off or fixed.

**There are similarities in the software layer. People take an operating system and assume that it has a reasonable set of features and mostly works. They don’t immediately go through the entire operating system loadout wondering, ‘Should I delete Power-Shell? Is it possible to write a virus in embedded macros?’ They assume it’s all well-intentioned stuff with a purpose, but it’s not accidentally dual-purpose.**

On the hardware side, a lot of what we see is vendors making it as easy as possible for engineers to use their chips. They create a bunch of reference code—samples of code designed to show off the features of a chip—so if an engineer says, ‘We need to use encryption in the...
chip,’ they’ll use whatever sample code was written by the vendor to work with [the] particular module on that chip. The problem is that those pieces of code are proof of concept, not production-quality code. It has disclaimers: ‘This should not be used in a product.’ But engineers take these chunks of code and slap them in, trusting that they are right. Sometimes it is written by interns, sometimes it is written to just show how to use the hardware model, and sometimes it is well-written. It’s the same problem: People are trusting code, and hardware, that was not vetted for security.

When I start developing a product that has a microcontroller, I’ll go through the data sheet and, as part of my start-up code, I disable every peripheral that I don’t need. Most people will just take whatever they’re given and let it run; that way, there may be things they didn’t ask for—open ports, configuration issues, things that haven’t been locked down. It’s just human nature nowadays: ‘It doesn’t need to be internet-connected, but I may as well leave that in.’

**Your approach is more expensive. You have to actually understand what you’re doing instead of taking the shortest path.**

It all boils down to managing the entry points into the system. And with today’s systems, we can’t rely on our ability to control the entry points.

**That’s not a cheerful note to end on.**

There are edge cases where progress is being made. You do have a lot of chip vendors that are starting to take security more seriously, and they’re making things better for the general populace. You’ll always have governments and high-end individuals that can break into things, but they’re making it to a point where engineers don’t have to understand security—it’ll work well enough. We are seeing little steps being taken, and even though there are so many potential underlying threats, if you look at the history of the last five or 10 years, there are lots of things that you can do that make your systems better.

**MARCUS J. RANUM** is a world-renowned expert on security system design and implementation. He served as senior strategist and CSO at Tenable Network Security. He has held computer and network security positions at Network Flight Recorder, a company he founded; TruSecure Corp.; V-One; Trusted Information Systems; and DEC.