SECURITY AT THE SPEED OF BUSINESS | SPRING 2019

CSO

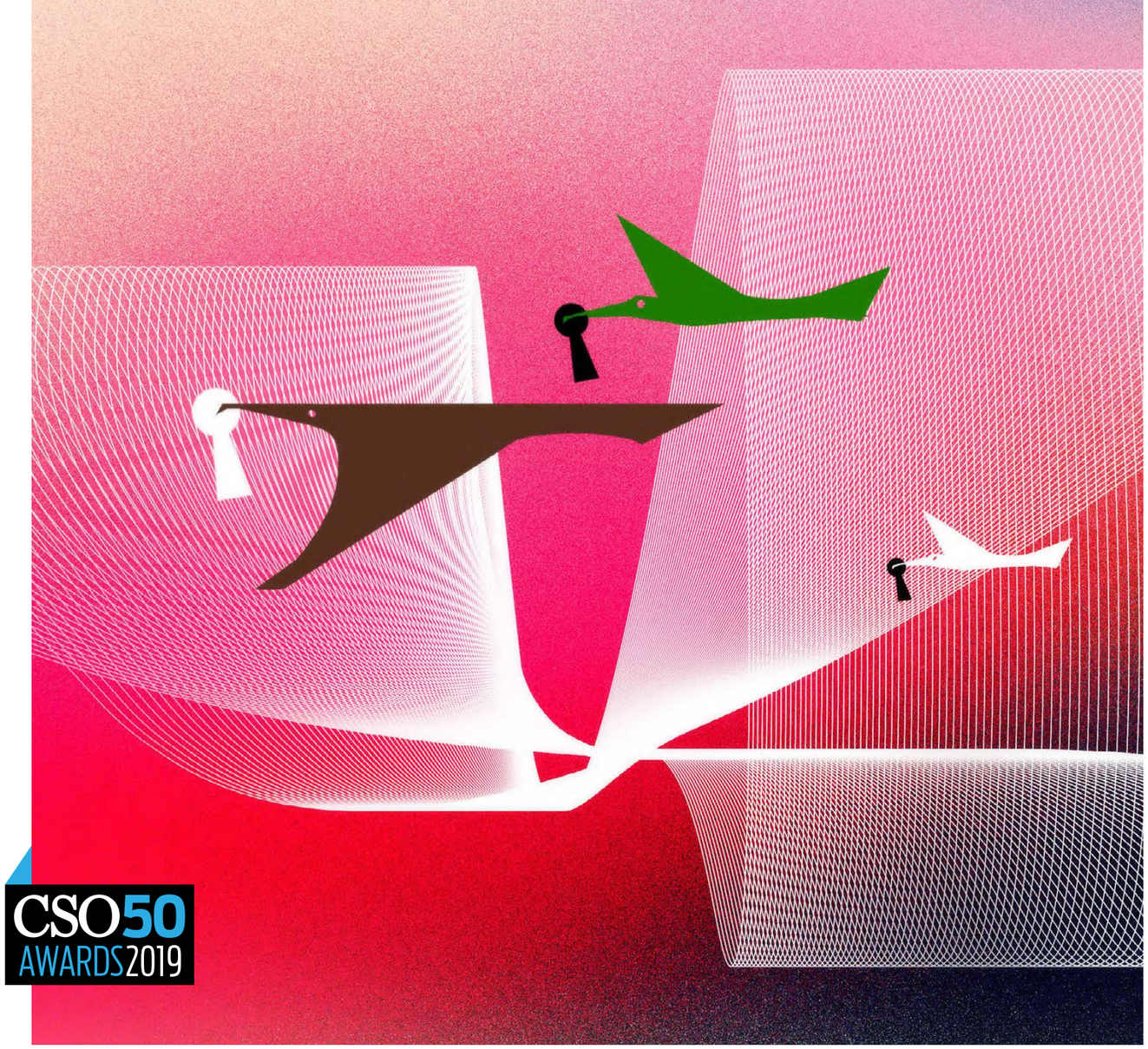
FROM IDG

Seeding Security IN THE Cloud

CSO50 AWARDS 2019

CSO50 award-winning companies *are rising to the cloud security challenge and finding new ways to protect data and assets.* **BY JAIKUMAR VIJAYAN**

Inside



[COVER STORY]

Seeding security in the **cloud**

BY JAIKUMAR VIJAYAN

CSO
FROM IDG

EDITORIAL

EXECUTIVE EDITOR
Amy Bennett

ART DIRECTOR
April Montgomery

SENIOR EDITOR
Michael Nadeau

SENIOR WRITERS
Lucian Constantin, JM Porup, Dan Swinhoe

CSO EVENTS

SVP/PUBLISHER
Bob Bragdon

IDG COMMUNICATIONS, INC.

PRESIDENT
Kumaran Ramanathan

US PRESIDENT
Charles Lee

FOUNDER
Patrick J. McGovern (1937-2014)

FOLLOW US ON ...

Twitter | *twitter.com/csoonline*
Facebook | *www.facebook.com/CSOonline*
LinkedIn | *www.linkedin.com/company/csoonline*

CONTACT US

www.csoonline.com/about/contactus.html

BRIAN STAUFFER / ALPHASPIRIT / D-KEINE / LIUZISHAN / GETTY IMAGES

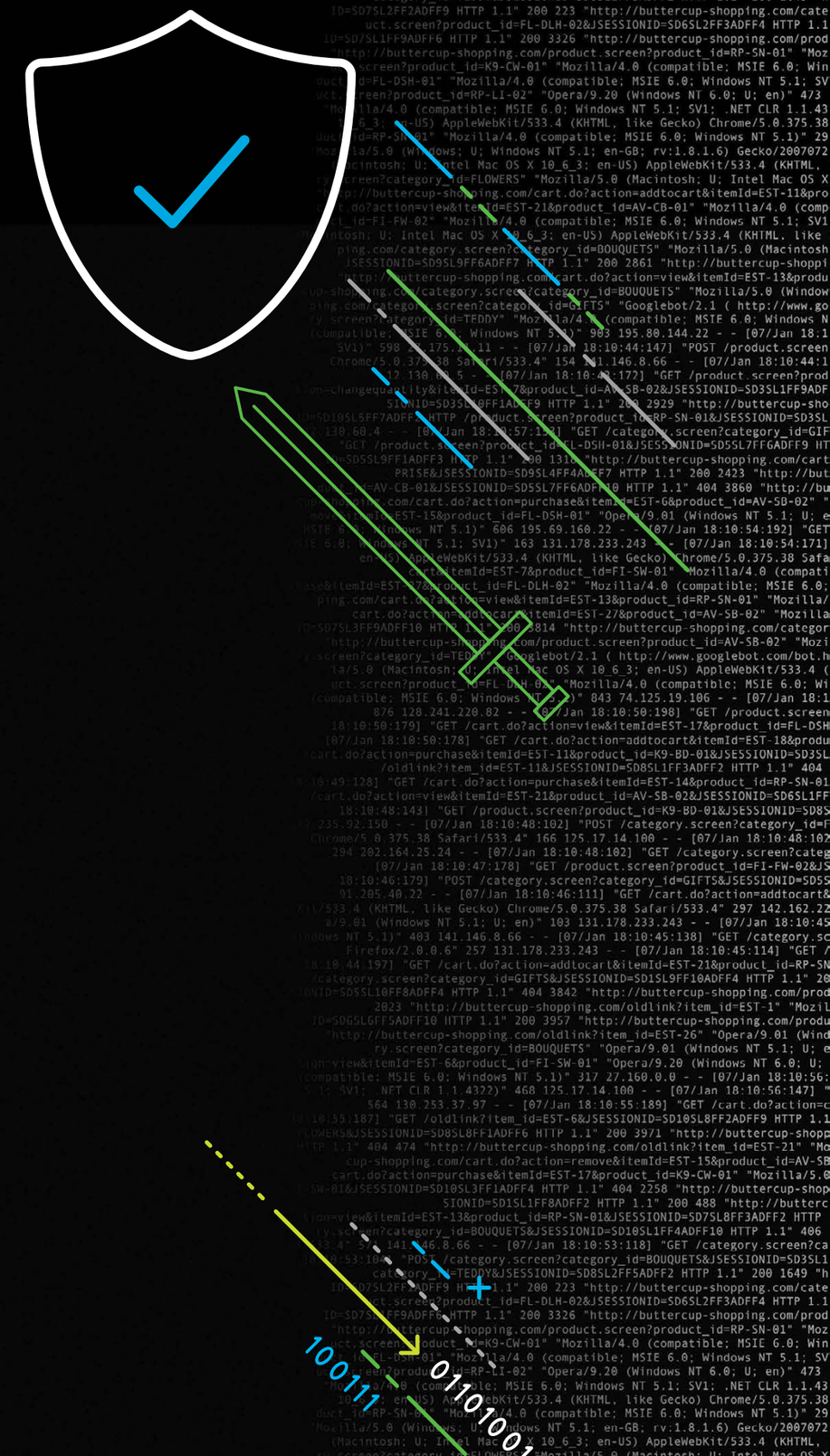
WEAPON OF A SECURITY WARRIOR.

Congratulations to our customers honored at CSO50 for security projects and initiatives that have delivered outstanding business value and thought leadership.

What can you do with Splunk? Learn more at **splunk.com**

splunk>

Listen to your data.®



How (and why) to build digital trust

Earning customers' trust translates to better customer acquisition, greater customer loyalty and more revenue. Here's how to do it. **BY DAN SWINHOE**

DIGITAL TRUST is the measure of consumer, partner and employee confidence in an organization's ability to protect and secure data and the privacy of individuals. It can be a valuable commodity for companies that earn it, and it is starting to change the way management looks at security.

A recent report on digital trust from CA Technologies, conducted by Frost & Sullivan, shows that taking security and privacy seriously can have a

ALPHASPIRIT / GETTY IMAGES

positive financial impact beyond avoiding costly breaches.

"Trust is one of the things that permeates across the whole business," says Stephen Walsh, senior director of solution sales at CA. "It is the bedrock of business, and without it, organizations are going to struggle to keep their existing customers, gain new customers or enter new markets."

> **Trust is one of the things that permeates across the whole business. It is the bedrock of business,** and without it, organizations are going to struggle to keep their existing customers, gain new customers or enter new markets.
>
> — **STEPHEN WALSH** (BELOW), SENIOR DIRECTOR, SOLUTION SALES, CA TECHNOLOGIES

Security as business enabler

The CA report shows that consumers with a high level of digital trust spend more, with 57 percent of those respondents increasing online spending over the past 12 months versus 43 percent of consumers with low trust.

"Quite a lot of people in the past have viewed security as kind of an incumbent, something that you have to get over," says Walsh. "The more boards think of security as an enabler and a way of actually acquiring new customers and new business, the better off we will be."

If gaining trust is good for business, losing it can be costly. Half of organizations surveyed in the report acknowledged that they have been involved in a publicly disclosed data breach, and nearly all found that the breach had a long-term negative impact on revenues and consumer trust. On the customer side, half said they stopped using a company's services if the company was involved in a breach and instead moved to a competitor.

"If customers see organizations who don't have that security, they're going to vote with their wallets and go somewhere else where they do have that sense of security and building up that digital trust," says Walsh. "Thinking about it twice probably means you've lost the customer because they'll go somewhere else. If you have the perception from customers that you are doing your best to keep their data, assets, money, whatever it is, secure, that's how you build trust. The other side of that is that sometimes it can only take one breach or security issue to lose that trust you built up over a number of years with your customer base."

10 best practices for building trust

In late October 2018, professional services firm PwC released its Digital Trust Insights report, based on a survey of 3,000 business leaders worldwide. From that data, PwC compiled this list of opportunities to build trust in a digital business environment.

1 Engage security in digital transformation projects

While more than 90 percent of survey respondents reported that their digital transformation projects include security or privacy stakeholders, only 53 percent involved them from the start. The report recommends a security- and privacy-by-design approach.

2 Upgrade talent

PwC's survey shows that most businesses are not fully confident in their security and privacy workforce. Only 38 percent said they were "very comfortable" that those teams are adequate. The report recommends doing a talent and skills gap assessment and committing to putting the right people in clearly defined cybersecurity, privacy and data ethics roles.

3 Raise workforce awareness

Only 34 percent of respondents said they have security awareness training programs. The report encourages prioritization of awareness of security and privacy and how they can affect business objectives. Policies around data governance and access to IT assets should accompany those efforts.

ALPHASPIRIT / GETTY IMAGES

4 Improve communication with boards of directors

Although most respondents said their boards are informed of cyber and privacy risk strategies, only 27 percent believe their boards have adequate reporting on metrics in both areas. PwC recommends that organizations identify the types of measures that are obtainable and can be measured now and make sure those metrics address the needs of the stakeholders.

5 Tie security to business goals

Only 23 percent of survey respondents said they plan to invest in aligning business objectives and security strategy. Steps to take include embedding cybersecurity into new products or services, conducting risk and regulatory compliance assessments, conducting cybersecurity framework assessments, and refreshing cybersecurity strategies and plans.

6 Build lasting trust around data

Of all companies worth $100 million or more, only about half make significant investments in data governance, according to the survey. The report recommends implementing data governance programs that take both the value and sensitivity of the data into account.

7 Boost cyber-resilience

Fewer than half of medium to large companies said they are building resilience to cyberattacks and other disruptive events. Becoming cyber-resilient requires an understanding of the company's risk appetite around core business processes. The report suggests taking the differing views of risk that each key stakeholder (CEO, CFO, CIO, etc.) might have.

8 Know your enemies

Organizations should know where their most likely threats are coming from. According to the survey, financial services firms are more worried about state-sponsored hackers (33%), while consumer-focused businesses see cybercriminals as a key threat (50%). However, only 31 percent of respondents said they are confident they've identified which parties might attack their digital assets.

9 Be proactive in compliance

Staying informed and in compliance with global privacy and data protection regulations is a big challenge. Forty-one percent of respondents said it is a challenge just to be aware of the regulations that affect them. The report emphasizes the need to focus on awareness of new legislation and recommends operating to the highest regulatory standard across all the jurisdictions the business operates in.

10 Keep pace with innovation

New technology creates new risk. With the internet of things, for example, only 39 percent of respondents are confident they have adequate "digital trust" controls in place to manage security, privacy and data ethics. PwC recommends organizations prioritize the development of digital trust controls and stay abreast of security research around newer technologies. ◆

DAN SWINHOE *is a senior writer at CSO.*

Mobile security threats you should take seriously in 2019

Mobile malware? Some mobile security threats are more pressing. Every enterprise should have its eye on these issues. **BY JR RAPHAEL**

MOBILE SECURITY is at the top of every company's worry list these days—and for good reason: Nearly all workers now routinely access corporate data from smartphones, and that means keeping sensitive info out of the wrong hands is increasingly difficult. And the stakes are higher than ever: The average cost of a corporate data breach is a whopping $3.86 million, according to a 2018 Ponemon Institute report. That's 6.4 percent more than the estimated cost just one year earlier.

While it's easy to focus on the sensational subject of malware, the

TRAFFIC ANALYZER / GETTY IMAGES

truth is that mobile malware infections are incredibly uncommon in the real world—with your odds of being infected significantly lower than your odds of being struck by lightning, according to one estimate.

The more realistic mobile security hazards lie in some easily overlooked areas, all of which are only expected to become more pressing.

1 Data leakage

It may sound like a diagnosis from the robot urologist, but data leakage is widely seen as being one of the most worrisome threats to enterprise security. Remember those almost nonexistent odds of being infected with malware? Well, when it comes to a data breach, companies have a nearly 28 percent chance of experiencing at least one incident in the next two years, according to Ponemon's research.

What makes the issue especially vexing is that it often isn't nefarious by nature; rather, it's a matter of users inadvertently making ill-advised decisions about which apps are able to see and transfer their information.

"The main challenge is how to implement an app vetting process that does not overwhelm the administrator and does not frustrate the users," says Dionisio Zumerle, research director for mobile security at Gartner. He suggests turning to mobile threat defense solutions—products like Symantec's Endpoint Protection Mobile, CheckPoint's SandBlast Mobile, and Zimperium's zIPS Protection. Such utilities scan apps for "leaky behavior," Zumerle says, and can automate the blocking of problematic processes.

Of course, even that won't always cover leakage that happens as a result of overt user error—something as simple as transferring company files onto a public cloud storage service, pasting confidential info in the wrong place, or forwarding an email to an unintended recipient.

For that type of leakage, data loss prevention tools may be the most effective form of protection. Such software is designed explicitly to prevent the exposure of sensitive information, including in accidental scenarios.

2 Social engineering

The tried-and-true tactic of trickery is just as troubling on the mobile front as it is on desktops, and social engineering cons remain astonishingly effective.

A staggering 91 percent of cybercrime starts with email, according to a 2018 report by security firm FireEye. Phishing, specifically, grew by 65 percent over the course of 2017, the company says, and mobile users are at the greatest risk of falling for it because of the way many mobile email clients display only a sender's name—making it especially easy to spoof messages and trick a person into thinking an email is from someone they know or trust.

In fact, users are three times more likely to respond to a phishing attack on a mobile device than a desktop, according to an IBM study—in part simply because a phone is where people are most likely to first see a message. While only 4 percent of users actually click on phishing-related links, according to Verizon's 2018 Data Breach Investigations Report, those gullible guys and gals tend to be repeat offenders: The company notes that the more times someone has clicked on a phishing campaign link, the more likely they are to do it again in the future. Verizon has previously reported that 15 percent of users who are successfully phished will be phished at least one

more time within the same year.

"We do see a general rise in mobile susceptibility driven by increases in mobile computing overall [and] the continued growth of BYOD work environments," says John "Lex" Robinson, information security and anti-phishing strategist at PhishMe. More and more workers are viewing multiple inboxes together on a smartphone, he notes, and almost everyone conducts some sort of personal business online during the workday. Consequently, the notion of receiving what appears to be a personal email alongside work-related messages doesn't seem at all unusual, even if it may in fact be a ruse.

The delivery of VPNs needs to be smarter with mobile devices, as minimizing the consumption of resources—mainly battery—is paramount.

— **DIONISIO ZUMERLE,** RESEARCH DIRECTOR, GARTNER

3 Wi-Fi interference

A mobile device is only as secure as the network through which it transmits data. In an era where we're all constantly connecting to public Wi-Fi networks, that means our info often isn't as secure as we might assume.

Just how significant a concern is this? According to research by enterprise security firm Wandera, corporate mobile devices use Wi-Fi almost three times as much as they use cellular data. Nearly a quarter of devices have connected to open and potentially insecure Wi-Fi networks, and within the most recent month, 4 percent of devices have encountered a man-in-the-middle attack, whereby someone maliciously intercepts communication between two parties. McAfee, meanwhile, says network spoofing has increased "dramatically" as of late, and yet fewer than half of people bother to secure their connection while traveling and relying on public networks.

"These days, it's not difficult to encrypt traffic," says Kevin Du, a computer science professor at Syracuse University who specializes in smartphone security. "If you don't have a VPN, you're leaving a lot of doors on your perimeters open."

Selecting the right enterprise-class VPN, however, isn't so easy. As with most security-related considerations, a trade-off is almost always required. "The delivery of VPNs needs to be smarter with mobile devices, as minimizing the consumption of resources—mainly battery—is paramount," Gartner's Zumerle points out.

4 Out-of-date devices

Smartphones, tablets and smaller connected devices —commonly known as the internet of things (IoT)—pose a new risk to enterprise security in that unlike traditional work devices, they generally don't come with guarantees of timely and ongoing software updates. This is true

particularly on the Android front, where the vast majority of manufacturers are embarrassingly ineffective at keeping their products up to date—both with operating system updates and with the smaller monthly security patches—as well as with IoT devices, many of which aren't even designed to get updates in the first place.

"Many [IoT devices] don't even have a patching mechanism built in, and that's becoming more and more of a threat these days," Du says.

5 Cryptojacking attacks

A relatively new addition to the list of relevant mobile threats, cryptojacking is a type of attack where someone uses a device to mine for cryptocurrency without the owner's knowledge.

While cryptojacking originated on the desktop, it saw a surge on mobile from late 2017 through the early part of 2018. Unwanted cryptocurrency mining made up a third of all attacks in the first half of 2018, according to a Skybox Security analysis, with a 70 percent increase in prominence during that time compared with the previous half-year period.

Since then, things have cooled off somewhat, especially in the mobile domain—a move aided largely by the banning of cryptocurrency mining apps from both Apple's iOS App Store and the Android-associated Google Play Store in June and July, respectively. Still, security firms note that attacks continue to see some level of success via mobile websites (or even just rogue ads on mobile websites) and through apps downloaded from unofficial third-party markets.

6 Physical device breaches

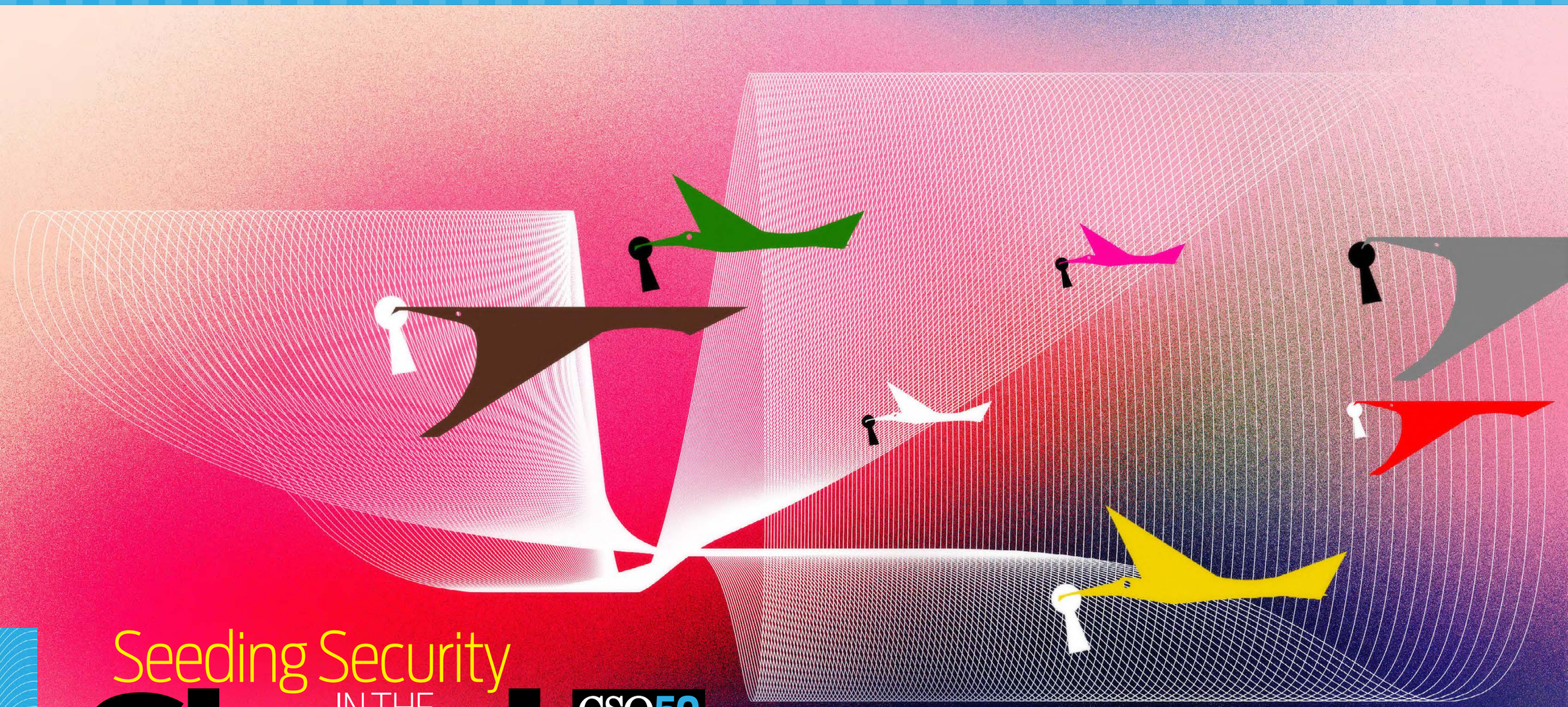
Last but not least is something that seems silly but remains a disturbingly realistic threat: lost or unattended devices.

Consider the following: In a 2016 Ponemon study, 35 percent of professionals indicated their work devices had no mandated measures in place to secure accessible corporate data. Worse yet, nearly half of those surveyed said they had no password, PIN or biometric security guarding their devices—and about two-thirds said they didn't use encryption. Sixty-eight percent of respondents indicated they sometimes shared passwords across personal and work accounts accessed via their mobile devices.

> **Many [IoT devices] don't even have a patching mechanism built in,** and that's becoming more and more of a threat these days.
>
> — **KEVIN DU,** PROFESSOR OF COMPUTER SCIENCE, DEPARTMENT OF EECS, SYRACUSE UNIVERSITY

The take-home message is simple: Don't make assumptions; make policies. You'll thank yourself later. ◆

JR RAPHAEL *is a regular contributor to CSO.*



Seeding Security IN THE Cloud

CSO50 AWARDS 2019

***CSO50 award-winning companies** are rising to the cloud security challenge and finding new ways to protect data and assets.* **BY JAIKUMAR VIJAYAN**

BRIAN STAUFFER

CLOUD ADOPTION is driving deep security changes at a growing number of organizations, though not always for the same reasons. For many businesses, the changes are a response to the fresh security risks posed by the rapid adoption of cloud technologies in recent years, particularly infrastructure as a service (IaaS) and platform as a service (PaaS).

Turner Broadcasting is one example. The $13 billion media giant recently completely overhauled its security program to manage new risks while it transitions to a cloud-centric infrastructure for delivering next-generation broadcasting and publishing services.

For other organizations, the security changes stem from the use of cloud services to deliver capabilities that they were unable to deliver previously. Here, the cloud is not the reason for the security overhaul but the fundamental enabler of it. Take Catholic Relief Services (CRS), a nonprofit that delivers humanitarian aid in some 100 countries, including several with little to no connectivity. After years of trying to revamp its global endpoint security environment via an on-premises system, CRS finally accomplished its goal last year using a cloud service from Microsoft.

Cloud requires new controls

For organizations that are concerned about the security implications of cloud adoption, the issue is usually more about ownership than technical vulnerabilities, says Pete Lindstrom, vice president of research, Enterprise/NextGen Security, at IDC. Accelerating adoption of cloud services has heightened fears over data ownership, access visibility and compliance. "It's a loss of control issue masquerading as a security issue," Lindstrom notes. "What you are doing with the cloud is subordinating your technical controls to your business controls."

Gartner expects that demand for IaaS and PaaS offerings from enterprises engaged in digital transformation and other large initiatives will exceed $206 billion

What you are doing with the cloud is subordinating your technical controls to your business controls.

— **PETE LINDSTROM** (ABOVE), VP OF RESEARCH, ENTERPRISE/NEXTGEN SECURITY, IDC

IDC

this year. There's considerable concern that the speed of migration of business critical workloads to these environments will heighten security risk for businesses and necessitate new security measures.

According to the Cloud Security Alliance (CSA), over the short term, mistakes that enterprises make when migrating workloads to the cloud—like exposed storage buckets, elevated user privileges and misconfigurations—have begun posing a graver threat to data than any inherent cloud security defects.

Legacy mistakes creep into the cloud

The same system management mistakes that organizations have been making on premises in terms of inaccurate asset inventories, unpatched systems, failure to maintain configuration standards and over-privileged accounts are creeping into the cloud, says John Pescatore, director of emerging security trends at SANS Institute. In practice many IT operations deficiencies are just continued across to the cloud, he says.

Enterprises are responding in different ways. One major trend that CSA expects is the growth of cloud automation and monitoring tools for helping administrators identify security issues and orchestrate responses across a wide variety of cloud instances. Turner, for instance, has implemented tools that give it real-time visibility into the security and compliance status of its cloud assets so the security team can detect and respond to issues faster.

Improved models for cloud architectures, continuous deployment and DevSecOps are also becoming key to improving the cloud security experience, according to CSA. So, too, is the notion of a shared responsibility model that articulates which control objectives should be the responsibility of the provider, which control objectives are the responsibility of the customer and which control objectives are the responsibility of both, says Jim Reavis, CEO of CSA. The model recommends an approach where enterprises treat cloud services as organizational assets and develop a risk-based approach to assessments using available baseline standards, he notes.

> **Because cloud tends to operate on the basis of standards,** one finds a baseline of security capabilities is virtually always available.
>
> — **JIM REAVIS** (ABOVE), CEO, CLOUD SECURITY ALLIANCE

Opportunities for better security

A growing number of companies are taking advantage of the transition to IaaS to change processes and procedures to actually make security better, says Pescatore. "One example is being able to have a test or development environment that can be spun up rapidly to allow patch testing to take hours instead of days," he says.

Other organizations, like CRS, are tapping the cloud to deliver new security services. For these organizations, the same flexibility, ease of access and cost benefits that are driving broader cloud adoption are driving the use of the cloud to enable better security.

"Public cloud providers collectively spend billions on securing their infrastructure, and consumers directly and tangibly benefit from this," says Matthew Chiodi, CSO of public cloud at Palo Alto Networks. For organizations operating large, on-premises environments, such services can help reduce the cost and effort involved in tasks like vulnerability management and patch management, he says.

"Public cloud providers shouldering the load for serious flaws not only reduce risk, but can also greatly aid an already overburdened IT workforce," Chiodi says.

Presently, cloud security adoption lags behind general cloud usage. But it is becoming more common for organizations to move workloads to the cloud specifically to bolster security. One example is log management and forensic analysis, both of which can be done much more efficiently with the elasticity of the cloud, Reavis notes.

"Because cloud tends to operate on the basis of standards, one finds a baseline of security capabilities is virtually always available," Reavis says. "Strong authentication is a common example of something that is straightforward to deploy in cloud relative to legacy technology." ◆

> **Strong authentication** is a common example of something that is **straightforward to deploy in cloud** relative to legacy technology.
>
> — **JIM REAVIS,** CEO, CLOUD SECURITY ALLIANCE

Read on to see how three 2019 CSO50 award winners are finding security success in the cloud. >>>

When **Windows security** is truly a matter *of* life or death

A COMPROMISED SYSTEM at humanitarian aid provider Catholic Relief Services (CRS) could endanger lives, yet regular Windows patching was next to impossible in some places. Information security director Joel Urbanowicz explains how a cloud solution provided centralized management of updates.

Most companies measure the consequences of a serious data security incident in terms of financial loss, brand damage and disruption to the business. The stakes are a lot higher at CRS, a U.S.-based nonprofit that provides humanitarian services to people in about 100 developing countries in sub-Saharan Africa, Central America, Asia and other parts of the world. Data from its computers in the wrong hands can literally mean the difference between life and death for some beneficiaries of CRS in regions where groups like the jihadist Boko Haram operate.

> We had an audit tool, but **we had no way to actually go out and remediate** [other] than asking [users] very firmly.
>
> — **JOEL URBANOWICZ** (ABOVE), DIRECTOR, INFORMATION SECURITY, CATHOLIC RELIEF SERVICES

To shore up data security, CRS in 2017 decided to implement a cloud-based system for centrally managing and enforcing security policies across its more than 6,000 Windows devices globally. One of the primary goals of the effort was to ensure that the devices—which contain everything from HR information to donor and beneficiary data—receive Windows security updates in a timely manner.

Mundane as that task is for most organizations, for CRS, it was a monumental challenge, says Urbanowicz. A vast number of the devices in the CRS network are in resource-limited locations with extremely challenging operational

environments that include volatile and dangerous political conditions, travel restrictions, severe shortage of skills and appallingly slow network connectivity.

The infrastructure challenge

Sometimes, the available bandwidth in areas where CRS operates is just 96Kbps per device and the best response times are in the 500-millisecond range. Attempting to download a Windows update in those conditions was a huge challenge prior to the cloud system, Urbanowicz says. "We were cratering our bandwidth constantly through Windows system updates," he notes.

CRS's existing on-premises platform wasn't designed to traverse the open internet, so delivering security patches and anti-malware protection from a central location was practically impossible. Most of the patch management was handled at the local level in a highly non-standard manner with little oversight. Fewer than 40 percent of the Windows devices that CRS staffers used had current patches at any given time, and even that number—self-reported by local offices—was mostly non-verifiable. "We had an audit tool, but we had no way to actually go out and remediate [other] than asking them very firmly," Urbanowicz recalls wryly.

> The real innovation was the **multicultural, geographically disperse team** that came together to enact this change across the agency.
>
> — **JOEL URBANOWICZ,** DIRECTOR, INFORMATION SECURITY, CATHOLIC RELIEF SERVICES

Stepping up security with a centralized cloud

The centralized cloud-hosted system that CRS implemented to address these issues is based on Microsoft's Intune Windows device management platform. It supports centralized services such as policy configuration and enforcement, OS patching, custom application deployment and endpoint protection.

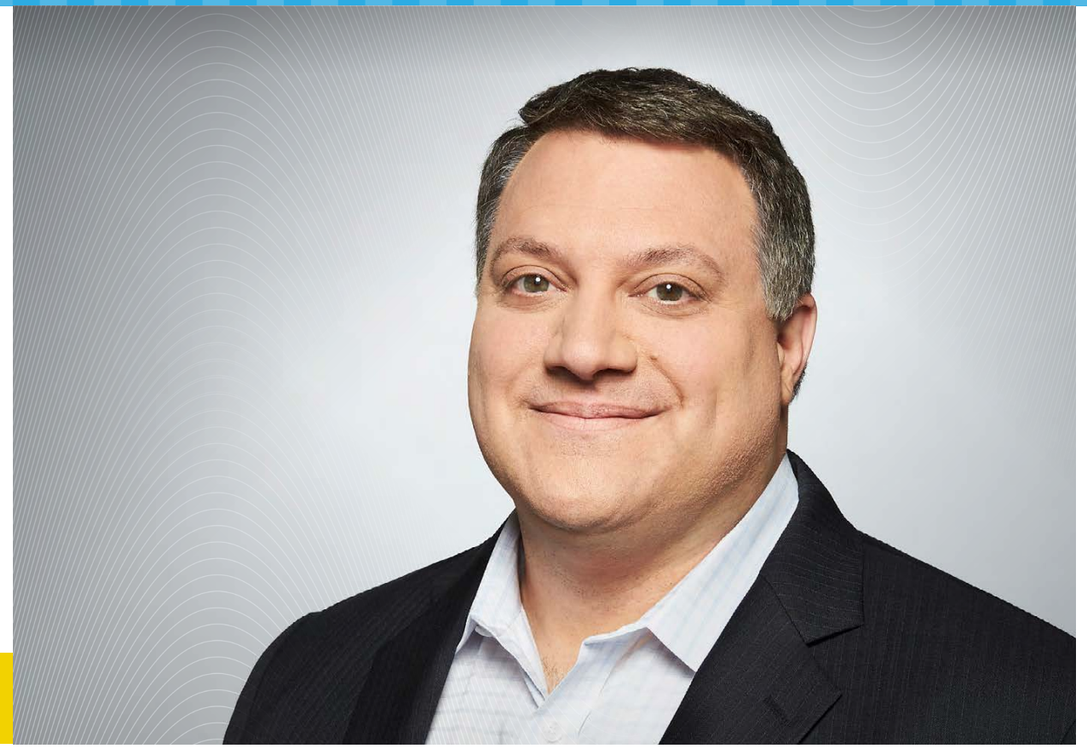
An Intune feature that allows CRS to cache Windows security updates has been especially useful because offices in different countries can now get their updates directly from their local country cache instead of having to pull it down over the internet. The bandwidth savings have been huge. Previously, a Windows update would chew up upwards of 80 percent of the available bandwidth in places like the Democratic Republic of Congo, Benin and certain other regions. The cloud system has allowed CRS to reduce consumption by 57 percent. "Deploying a multigig image for Windows 10 to an IT manager in South Sudan wasn't possible," Urbanowicz says. "They couldn't connect long enough to pull the patch down."

The proportion of CRS systems with current Windows security updates has more than doubled from 39 percent in July 2017 when the cloud project started to more than 90 percent today.

The cloud system has engendered other benefits as well. Prior to implementing the cloud system, 60 people were engaged in patch deployment. Now a team of four operating out of India, Zimbabwe and the U.S. handles the task across the CRS network, freeing the rest to focus on more productive tasks, including third-party application patching and new application deployment. And, because CRS can now centrally manage the desktop environment, the agency has been able to save costs by decommissioning the local update servers it previously needed to maintain.

"The real innovation was the multicultural, geographically dispersed team that came together to enact this change across the agency," Urbanowicz says. "It took every one of those 60 people to get us to where we are, allowing for the team of four to maintain it moving forward." ◆

Media company tunes in *to* cloud security standards



TURNER BROADCASTING'S Cloud Security Program allows it to minimize risk associated with adopting new technology. Senior vice president and CISO Peter Chronis details how the program has drastically reduced vulnerabilities across Turner's cloud stack.

Reimagine TV is a highly cloud-centric initiative by $13 billion media giant Turner Broadcasting to deliver custom programming and advertisements over traditional broadcast and digital platforms. Instead of allowing security concerns to hamper innovation, Turner's information security office and cloud architecture teams took advantage of the initiative

> The goal [was] to help **influence technology and business decisions** without introducing new, unmanaged technology risks to the business.
>
> — **PETER CHRONIS** (ABOVE), SVP AND CISO, TURNER BROADCASTING

TURNER BROADCASTING

to fundamentally improve the company's cloud security posture.

Turner's Cloud Security Program started a few years ago, around the same time the media company began deploying new cloud-centric capabilities to support its next-generation broadcasting and publishing initiative. The idea was to ensure that security risk was addressed at the same time cloud technologies were adopted, says Peter Chronis, senior vice president and CISO at Turner. "The goal [was] to help influence technology and business decisions without introducing new, unmanaged technology risks to the business."

Like many companies, Turner—the owner of CNN, TBS/TNT, Cartoon Network and other properties—needed a new way to better manage cloud security, architecture and spending prior to the security initiative. With the cloud being central to Reimagine TV and to new business opportunities, Turner's security and IT teams began working more closely together to define baseline security standards and promote secure development practices across the organization. The company embraced a DevSecOps security approach that integrated cloud operations, security and general IT best practices.

> We had opportunities to **build security and compliance capabilities into our cloud environments** that were not available to us in our legacy technology environments.
>
> — **PETER CHRONIS,** SVP AND CISO, TURNER BROADCASTING

Setting new standards

Turner's Cloud Security Program has yielded new standards that set minimum requirements for asset and risk management, configuration, endpoint protection, incident detection, incident response, compliance and several dozen other security controls.

To enforce the standards, Turner implemented compliance-monitoring capabilities that provide real-time visibility into the security status of more than 250 Turner cloud accounts on Amazon Web Services (AWS) and more than 7,500 cloud controls points. Separate intrusion detection and vulnerability scanning tools from Alert Logic provide similar real-time visibility into the security health of thousands of Turner cloud hosts on AWS.

"Real-time security policy compliance reporting is the gold standard," Chronis notes. "It tells you when and where you are meeting your corporate standards and gives you the ability to address gaps before an incident or an audit."

By having the ability to quickly spot and act upon deviations from minimum standards, Turner is able to handle cloud risk more confidently, Chronis says. Turner is currently in the process of deploying the cloud security standard to protect its assets on Microsoft Azure and Google's Cloud platform.

Building in security

Turner's cloud security initiative has yielded multiple benefits. "We had opportunities to build security and compliance capabilities into our cloud environments that were not available to us in our legacy technology environments," says Chronis.

At a high level, the program supports Turner's strategic mission of delivering 100 percent uptime broadcast networks and digital properties and has helped Turner reduce overall cloud spend. The emphasis on secure development and deployment has reduced the number of software vulnerabilities across Turner's cloud stack by more than 90 percent.

Data from Turner's compliance monitoring and vulnerability scanning tools enables its security operations center to have real-time visibility into potential security issues such as exposed cloud storage resources and high-risk account configurations. "We had to carefully embed resources strategically tied to key business initiatives in order to jump-start our program," Chronis says. "We created interactive training programs, standards and lots and lots of collaboration along the way." ◆

Taking a public health approach *to* endpoint protection

PEDIATRIC HEALTHCARE SYSTEM

Children's Health leverages the cloud to provide data and network protection resources to smaller

> **Clinics are not security companies.**
>
> — **WILL LONG** (ABOVE), CSO, CHILDREN'S HEALTH

partners. CSO Will Long describes how this benefits everyone.

Protection for all

"Clinics are not security companies," says Long, explaining his organization's decision in 2016 to launch CyberAid, an initiative to give small healthcare providers access to a fully managed endpoint protection service.

"CyberAid grew out of the recognition that clinics and doctors' offices do not have the expertise or resources to implement and maintain proper cyber-protection technologies," he notes.

Children's Health is one of the leading pediatric healthcare providers in the U.S. It currently hosts numerous small physician practices—entities with fewer than 75 employees—on its electronic medical records (EMR) system.

Children's Health launched CyberAid in collaboration with HITRUST, the developer of a widely used risk and compliance management framework for healthcare data, to address concerns over the ability of these small providers to properly protect data with their limited security resources. Many did not have the ability to select, acquire, implement and operate the security controls needed to properly protect against cyber-risks. With CyberAid, HITRUST is responsible for identifying and evaluating security products that healthcare organizations with limited resources can implement easily.

> CyberAid grew out of the recognition that **clinics and doctors' offices do not have the expertise or resources** to implement and maintain proper cyber-protection technologies.
>
> — **WILL LONG,** CSO, CHILDREN'S HEALTH

Breaches on the rise

Breaches involving healthcare data have steadily increased in recent years at least partly as a result of security shortcomings. Data maintained by the U.S. Department of Health and Human Services' Office for Civil Rights shows over 400 breaches were reported in the past 24 months involving healthcare data belonging to over 12 million people. Nearly three dozen of the breaches involved hacking, unauthorized access or accidental disclosure of EMRs.

In launching CyberAid, Children's Health wanted to deliver an

endpoint and network protection technology that was integrated with the cloud and harnessed its shared computing and analytics infrastructure to reduce costs, Long says. The goal was to give smaller health providers a turnkey service with enterprise-level security protections at a cost that made sense to them and that someone else is responsible for monitoring and keeping up to date.

Under the initiative, clinics work directly with security vendor Trend Micro and HITRUST. Together, the two organizations have deployed a standard set of technology controls that clinics can subscribe to for a few hundred dollars per year per doctor. The endpoint protection service supports Windows, Mac OS X and mobile devices running Android and iOS.

"There is nothing for the clinic to select, as the program includes the endpoint product, network product and the remote monitoring reporting [technology]," Long notes. By keeping the technology simple and standard, the program benefits from scale and lower costs. "This frees the clinics to focus on patient care with the confidence that their cybersecurity needs are being actively monitored and addressed," he says.

identified threats on average per month across the clinics. Threats being stopped include ransomware and phishing attempts—two major contributors to security breaches in the healthcare sector recently.

"By tying these clinics into a centralized system, they all are protected better through automatic threat updates and feeds that allow their technology to block new threats faster," says Long. "The clinics do not have to update or do any manual updates or intelligence sharing." ◆

> By tying these clinics into a centralized system, **they all are protected better through automatic threat updates** and feeds that allow their technology to block new threats faster.
>
> — **WILL LONG,** CSO, CHILDREN'S HEALTH

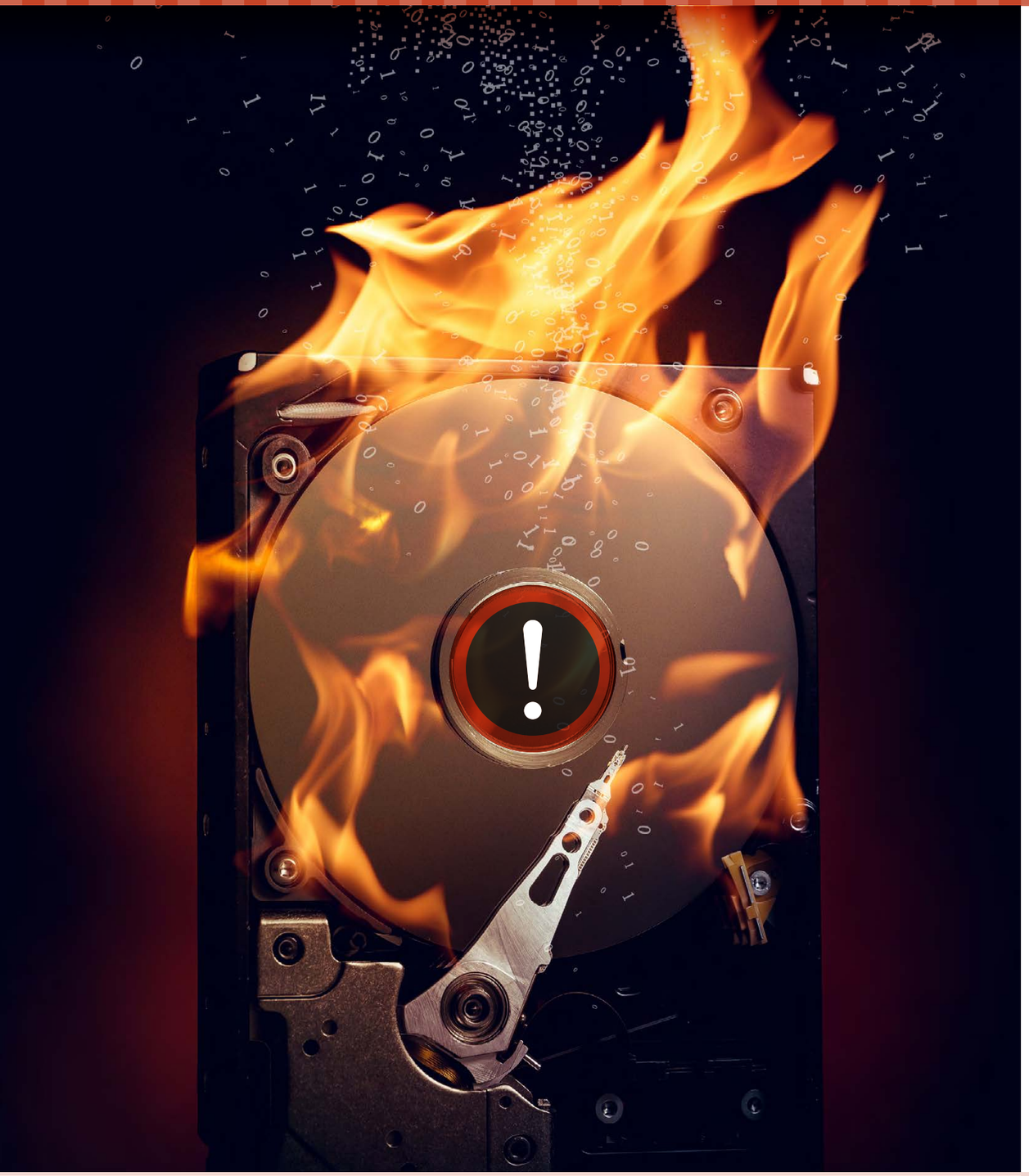
Affordable cyber-protection

Currently, all the clinics hosted on the Children's Health EMR system are signed up with CyberAid and have access to a class of cyber-protection they would not have been able to afford otherwise. The hosted service is blocking over 20,000

JAIKUMAR VIJAYAN *is a regular contributor to CSO.*

CSO50 2019 winners

- Accenture
- Adobe Inc. *[recognized for two projects]*
- ADP
- Aflac
- Allina Health
- Bank of America
- Bank OZK
- Black Knight Inc.
- Blue Cross NC
- Caesars Entertainment
- Catholic Relief Services
- Children's Health
- City of Phoenix
- City of Raleigh
- Cox Automotive
- Delta Dental Insurance Co.
- Dharampal Satyapal Ltd.
- DocuSign
- eClerx Services Ltd.
- Ellie Mae Inc.
- Fairfax County Government, Information Security Office
- Genpact
- HP
- IBC Bank
- Indiana University
- Innogy SE
- Internal Revenue Service
- Lear Corp.
- Lexmark International Inc.
- Microsoft
- Northwestern Mutual
- Nyhart
- Office of the Comptroller of the Currency
- Ottawa County Central Dispatch Authority
- Penn Medicine
- Polaris Alpha
- Premera Blue Cross
- PV Schools
- QuadReal Property Group
- Rogers Communications
- The AES Corp.
- The Maritime & Port Security ISAO Inc.
- The University of Oklahoma
- Turner
- Two Sigma Investments LP
- United Airlines
- United Nations Development Programme
- Verizon Communications
- Visa Inc.



6 things your disaster recovery plan should include

Natural and man-made disasters can knock out enterprise networks and data access without warning. With a good disaster recovery plan, you'll be better prepared for the unexpected. **BY JAMES A. MARTIN**

HURRICANES. TORNADOES. Earthquakes. Fires. Floods. Terrorist attacks. Cyberattacks. You know any of these could happen to your business at any time. And you've probably got a disaster recovery (DR) plan in place to protect your enterprise's data, employees and business.

But how thorough is your DR plan? When was it last updated and tested? Have you taken into account new technologies and services that can make it easier to recover from disaster? The follow-

D-KEINE / LIUZISHAN / GETTY IMAGES

ing are six things your IT disaster recovery plan should include.

1 An analysis of all potential threats

Your DR plan should take into account the complete spectrum of "potential interrupters" to your business, advises Phil Goodwin, research director of data protection, availability and recovery for research firm IDC. (IDC is part of IDG, which publishes CSO.)

You should then spell out a recovery plan for each scenario. For example, Goodwin says, "If there's a cyberattack that shuts down servers in D.C., do you have a transition plan for that scenario?"

Of course, not all scenarios are equally likely to occur. So as best you can, try to anticipate which potential disruptors are most probable. Sadly, cyberattacks are becoming "a more likely scenario" these days, Goodwin notes. So, you might want to give cyberattack planning precedence, he explains.

2 A business impact analysis

To effectively determine DR priorities, put each major information system through a business impact analysis (BIA), recommends Mark Testoni, president and CEO of SAP National Security Services.

A BIA "identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on business operations," according to Gartner.

"Completing a BIA for major IT systems will allow for the identification of system priorities and dependencies," notes Testoni. "This facilitates prioritizing the systems and contributes to the development of recovery strategies and priorities for minimizing loss. The BIA examines three security objectives: confidentiality, integrity and availability."

What behaviors will you need from your user community? What do they need to get up and running again after a disaster?

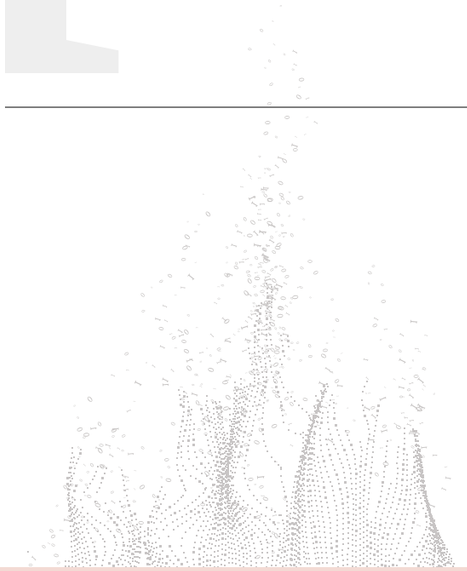
— **PHIL GOODWIN,** RESEARCH DIRECTOR, IDC

IDC

Testoni adds that a BIA helps establish priorities for your disaster recovery, business continuity, or continuity of operations plans. "A standard approach to developing a comprehensive disaster recovery plan is to first develop the policy, then conduct the BIA," he says. "After creating a prioritization with the BIA, contingency strategies are developed and formalized in a contingency plan."

Know what you plan to say, how much you plan to reveal, and how you'll reassure those who might be nervous of continuing business with your company.

— **JOHN IANNARELLI,** SECURITY CONSULTANT AND SPEAKER



3 A focus on people

A common mistake many organizations make in their DR plans is "too much focus on technology and not enough on people and process," Goodwin says. "IT is an enabler. Never forget you're not just recovering data and servers." He recommends thinking about how to build a DR plan in the context of your entire organization. "What behaviors will you need from your user community? What do they need to get up and running again after a disaster?"

Also, identify by name the critical people charged with responding to a crisis, says John Iannarelli, a security consultant and speaker and former member of the FBI Cyber Division. Make sure you have their email, cell and home numbers. Make it clear who will be called in to work during a crisis. Know who you'll call for help, such as law enforcement, and if possible, establish a relationship with authorities before a disaster strikes. Decide in advance who will speak to the victims, clients and employees in the event of a disaster. "Know what you plan to say, how much you plan to reveal, and how you'll reassure those who might be nervous of continuing business with your company," he adds.

4 Regular updates

Another big mistake organizations make is not updating their disaster recovery plans after changes are made to their internal systems,

such as major software updates, notes Mark Jaggers, a Gartner research director focused on IT infrastructure strategies. Your plan isn't complete unless it takes into account all the technologies, systems and applications currently in use.

Plus, there may be new technologies or offerings to come along since you made your DR plans. DR plans are based on assumptions about the processes and tools available at the time the plans are finalized. "But those assumptions can change significantly, as technology evolution is quicker than ever before and innovations spring from unlikely places," notes Milind Kulkarni, vice president of product management for network resilience company Veriflow.

"Advances in computer science, predictive algorithms and the availability of huge compute capacity at a reasonable price-point allow the emergence of new approaches and solutions to guarantee IT systems' resilience, uptime, availability and disaster recovery," Kulkarni adds.

> **Think of it as if your house were on fire.** What would you grab as you run out the door?
>
> — **JOHN IANNARELLI,** SECURITY CONSULTANT AND SPEAKER

For example, with services such as Amazon's AWS Snowball, organizations can transfer petabytes of business data to a dedicated, secure appliance on site. Once the transfer is finished, you ship the appliance to the AWS center of your choice, where your data is transferred into the cloud. AWS Snowball and others like it give organizations innovative, affordable new ways to ensure data redundancy, Kulkarni says—which is a foundation of any DR plan.

5 A priority list

"Identify what's most important," recommends Iannarelli. "Not everything in your business is worth saving or needs to be protected. Your proprietary information, of course, is. But any info that is for public release is not as important. Think of it as if your house were on fire. What would you grab as you run out the door?"

6 Regular practice drills

"Just having a DR plan isn't enough," warns Kulkarni. "The plan needs to be regularly tested, and people need to practice procedures, just like a school prepares its students for fire and emergency drills on a regular basis. If not regularly practiced, the plan is ineffective."

Don't wait

The biggest mistake most companies make is waiting until after a cyberattack or disaster to figure out what to do next, says Iannarelli. "In my 20-plus years with the FBI, I've never seen anyone fired from a company because of a data breach. But I have seen many people fired for their failure to respond properly to a breach." ◆

JAMES A. MARTIN *is a regular contributor to CSO.*

Resources

SPONSORED BY: | splunk>

DOWNLOAD HERE

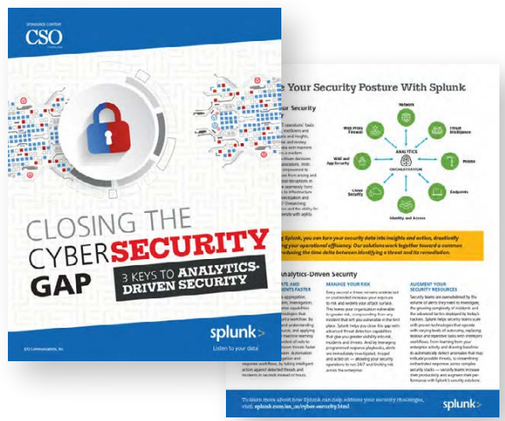
Aflac Adopts Splunk Platform for Analytics-Driven Security

■ Facing increased volume and velocity of security threats, Aflac needed a new analytics-driven security approach to protect its customers, nearly 10,000 employees and brand reputation. **The Splunk platform became the heart of its internal Threat Intelligence System (TIS).**

DOWNLOAD HERE

Data Secrets Revealed: A Collection of Security Customer Stories

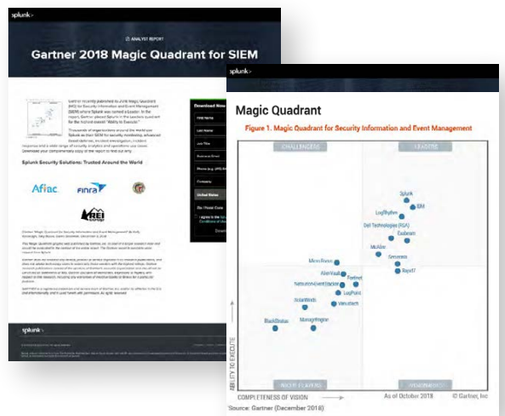
■ **"How did they do that?"** We've all seen the magic trick where the magician pulls a rabbit from a hat. Or a coin from someone's ear. Or makes someone disappear from a locked box. Splunk customers may not have rabbits, coins or magic boxes, but they do some amazing things. **Let us show you how.**



DOWNLOAD HERE

Closing the Cybersecurity Gap: 3 Keys to Analytics-Driven Security

■ Armed with the **3-step process** of [1] centralizing data, [2] automating and orchestrating, and [3] integrating and optimizing, organizations can continue running their IT departments and innovating for the future while at the same time handling the increasing workload around security operations.



DOWNLOAD HERE

Gartner 2018 Magic Quadrant for SIEM

■ Gartner recently published its 2018 Magic Quadrant (MQ) for Security Information and Event Management (SIEM), **placing Splunk in the Leaders quadrant for the highest overall "Ability to Execute."** Download your complimentary copy of the report to find out why.