CSO
FROM IDG

SPRING 2018

CSO50 AWARDS2018

RISKY BUSINESS

CSO50 AWARD WINNERS take security risk management to new heights **BY STACY COLLETT**

CSO 50 AWARDS 2018

RISKY BUSINESS

CSO50 AWARD WINNERS take security risk management to new heights

BY STACY COLLETT

Risk. Some might call it the new four-letter word in security. Security risk seems to increase in lockstep with every new technology innovation, business development and threat actor discovered. Today, company data resides in the cloud and on mobile devices and is connected

DERFLA/PIXABAY

to the internet of things (IoT). Threat vectors are multiplying, threatening companies' operations, customers and future financial stability.

The World Economic Forum ranked cyberattacks the 12th largest risk to doing business in 2017, ahead of natural catastrophes, which ranked 20th.

What's more, security leaders are constantly challenged to communicate ever-changing security risks to executives and boards of directors — and deal with the fallout should the risk exceed their appetite.

Nearly 20 percent of this year's CSO50 Award winners took on security risk and compliance projects, tackling security risk associated with outsider threats, third-party vendors, medical devices, compliance and keeping university systems open but safe for thousands of students. These are just a few of their stories.

Managing third-party risk

Allstate Insurance Co. knows all about managing risk, but the Northbrook, Ill.-based company started taking a closer look at how it assessed and mitigated security risks associated with its approximately 2,000 third-party suppliers in 2016 after the high-profile Target breach was traced to credentials stolen from a heating and cooling vendor that had access into the data center.

"It's an issue that's been front and center at Allstate for several years now, but with the speed that technology and the business environment are moving, it continues to rise toward the top of things that we're concerned about and our shareholders are concerned about," says Jeffrey Wright, Allstate senior vice president and CISO.

The Target breach renewed a string of topics for Wright and his team: "How do you provision access to vendors? Do you allow them to come in, and from where? How do you evaluate the security controls in their environment? It's a huge ecosystem," he says.

Complicating matters further, Wright adds, is that "we see complexity in our ecosystem when you think about SaaS and our own cloud service providers and platform service providers. So what about our vendors? How many vendors do we use that may also implement cloud-based solutions or rely on what we call fourth parties?" The team's old system for assessing security risk wasn't going to shed light on these big questions, he says.

To improve its existing supplier security risk management function, Wright's team — along with members from Allstate's information security, privacy, procurement and RSA Archer teams — rebuilt the procurement, privacy and information security process to incorporate industry best practices, frameworks and procedures.

The team rebuilt each area's respective process while automating each task into its RSA Archer risk management system and calculating the inherent and residual risk.

Wright worked with Allstate's privacy team to objectively evaluate each contract and score it, based on the high volume vs. low volume of data shared, critical vs. noncritical data, and whether the ven-

Jeffrey **WRIGHT**
Allstate senior VP and CISO

dor provides core vs. noncore functions. The scores were fed back into procurement, so when contracts are written, writers know what contractual language is needed to meet Allstate's security requirements. The team also added a non-negotiable term to all of its supplier contracts: the right to perform on-site audits.

Next, the team added SecurityScorecard technology to Archer to assess the security posture of all suppliers. It continuously monitors the suppliers and alerts Allstate to any deviations in their security.

The security risk transparency and new contract requirements did take its toll on a few vendors, Wright says. "We've probably lost some vendors along the way," though he declines to specify how many. "With a couple of vendors, it has come down to the eleventh hour. We're not going to budge on what our expectations are."

In seven months, Allstate's security risk management program went from a subjective, paper-based four-person team to one that is incorporated with its procurement, legal and data privacy departments, Wright says. It also provides visibility into third-party security risk up to the executive vice president level and has reduced a supplier's onboarding time from 132 days to 87.

Perhaps more important, Wright says, the new program provides "sophistication" in how Allstate determines which vendors it uses, how they are utilized and the real cost of outsourcing or using a third party to provide a service.

"It provides a tremendous amount of insight into the way your business operates, and [as a security leader], it puts you in a fantastic position as someone who can help the business operate more efficiently," Wright says. "I don't mind not being the guy saying no."

Starting from scratch

I**T and manufacturing** environments are no longer considered two different worlds at Kimberly-Clark Corp. As the Dallas-based manufacturer expands digital transformation of its 90 core manufacturing facilities and 120 global offices, it has had to build a security risk management program from scratch. Four years ago, security risk management at the company was nonexistent, says Corey Jackson, interim CISO. "Everything from true security operations to compliance, policy and threat intelligence is all still in its infancy."

It was also important to be able to communicate security risk to the board of directors in a language members could understand, Jackson says. "We wanted to make sure we had the right controls in place, to show that true business-related risk ties to products that generate revenue and show how that technology risk, if not managed correctly, could interrupt that revenue stream."

In February 2017, the company launched development of a corporatewide risk management framework, called the Global IT Risk Management program, to better assess and control threats to its critical information systems and reduce its risk profile.

The company leveraged best practices established by the National Institute of Standards and Technology (NIST) to develop and operationalize a framework for reducing risk to critical information systems. Next, it established governance bodies, including the Risk Assurance Committee, Global Risk Oversight Committee, IT Risk Oversight Committee, and IT Risk Working Group to maintain oversight of risks and explicitly use risk analysis in making decisions.

> “Everything from true security operations to compliance, policy and threat intelligence is all still in its infancy.”
>
> —COREY JACKSON

Corey **JACKSON**
Kimberly-Clark Corp., Interim CISO

The CISO’s office then had to take a security inventory of all its systems and vendors, an arduous task considering that many of its 90 manufacturing facilities have two to four variations of a particular technology deployed based on what they’re manufacturing, and 15 percent of systems are considered “hard-core legacy” manufacturing systems that can’t easily be replaced or modified because of their specialized duties. “So, we have to layer in more lines of defense,” Jackson says. The team established three risk levels and associated risk hierarchy business rules, including accountability/ownership, access control and governance.

The project’s linchpin was the addition of RSA Archer security risk management software, which takes all of the systems’ information and provides security analysis, response, and monitoring and controls. It has improved the consistency of risk management, as well as transparency and agility, Jackson says.

Within three months of full execution, the company closed 95 percent of 246 external-facing website vulnerabilities. Within four months, IT risk analysis information was used to brief Kimberly-Clark’s CEO, C-suite members and board of directors to demonstrate risk coverage. The CIO also uses the program to track the most concerning IT risks. Risk updates are provided to senior leaders on a regular basis, and risk responses are coordinated with stakeholders to ensure a synchronized approach.

The most important benefits of the projects for Jackson are greater security awareness and having a way to translate security risk into an actionable result. “Now, with the processes, focus and tools, we clearly have a way to do that, and it’s utilized daily,” he says. “We’re now seeking individuals outside of IT — in audit, the controller and chief risk officer — to think the same way we do about risk and to utilize the same solution to now paint a bigger, more focused risk picture collectively."

Uniting a university

Universities always struggle to strike a balance between access for its students and cybersecurity across all campuses. For the University of California, the challenge became more pressing and complicated in December 2015, after an attack on a system storing the Social Security and bank account numbers for 80,000 current and former faculty, staff, students and vendors.

"Our leadership realized we had to take a different tack on trying to manage cyber-risk," says CISO David Rusting. "Cyber-risk is much broader than [an attack]; it encompasses legal, ethical, risk services and IT issues combined. We felt that awareness needed to be raised to a much more senior level, and we needed to have a much more consistent and coordinated approach."

Among its unique challenges was the fact that the university's 10 campuses and five health systems were highly decentralized and independent across many functions, including security. Rather than a traditional command-and-control structure, "we function in a shared governance environment as a convener and coordinator of security functions in these two very different environments," Rusting says.

Doing something in a consistent and coordinated fashion among many entities would be difficult, but with the right leadership support, the university united and worked through the process in a collaborative way.

Together, they launched the Cyber-Risk Management Initiative, a program based on five core pillars of cyber-risk management, including governance, risk management, modernizing technology, common solutions and cultural change. These pillars supported all aspects of cyber-risk management and were used to drive cyber-risk reduction across all 10 campuses and five health systems.

David **RUSTING**
University of California, CISO

In a series of firsts for the university, each location within the university has a designated executive who reports to their chancellor on issues of cyber-risk and is empowered to drive cyber-risk efforts across their location. Consistent risk assessments were conducted across all 15 locations. Threat detection and identification was deployed at all locations, another first for a higher education and healthcare organization of UC's size and complexity.

Though health systems generally require more stringent security controls than college campuses, "a lot of basic controls in security are horizontal," Rusting says. "Managing risk levels up and down depending on the nature of data, context and the regulations that surround it — that's the risk-based activity that we go through. It's a bit of hard work, but it's worth it."

The university also leveled the security playing field by filling technology gaps at campuses with fewer security investments, including adding FireEye threat detection software at most locations, to help campuses meet the sophisticated threats they're now facing.

The results: UC's ability to detect and respond to threats across all campuses and health systems went from days and weeks to just a few hours. Cybersecurity training was mandated, with nearly 90 percent compliance in the first year and 95 percent compliance in the second year. A leading-edge information security policy was developed, and notifications due to breaches dropped significantly.

Measuring maturity

Bank of the Ozarks had no appropriate mechanism to assess its cyber-risk posture, nor were there any appropriate mechanisms to assess the efficacy of the bank's cybersecurity controls. CISO Brian Fricke knew that the Federal Financial Institutions Examination Council (FFIEC) had a cybersecurity assessment tool to help institutions identify their risks and determine their cybersecurity preparedness, but from a regulatory perspective, it wasn't very effective in linking inherent risk and residual risk based on the controls the bank has implemented. So, Fricke developed a Cybersecurity Risk and Control Maturity Assessment program that combines traditional risk and maturity assessments and unifies the two very different worlds of risk and cybersecurity.

"We figured out how to marry up the risk with the 149 critical security controls and to do a maturity assessment so I can communicate it to the board and to regulators, [to] whom I have to express the importance of the control gaps," Fricke says.

The process, in spreadsheet form, includes a risk assessment section and a maturity assessment, with individual tabs for each of 20 critical security control areas. In the control maturity assessment, each control needed an objective definition, a control owner, a description of the actual control as implemented in the organization, and the control's maturity assessment, which is based on four criteria: control defined in policy, control implemented, control automated, and control reported.

The cyber-risk assessment defines a Committee of Sponsoring Organizations-based risk assessment model, which is used in other areas of the organization. The team defined 20 top-level cyber-risks that the 20 critical security controls specifically address, and those received an inherent risk rating based on impact and likelihood. That data is linked to the control maturity assessment to determine an objective residual risk.

With the organization's overall level of inherent risk objectively defined, it is now able to focus on the most important controls. So far, it has implemented 122 of the 149 critical security controls, a 66 percent improvement from 2016. ♦

Brian **FRICK**
Bank of the Ozarks, CISO

Stacy Collett is a contributing writer for CSO.

INNOVATION *takes center stage*

The annual **CSO50 Awards** recognize innovative security projects that demonstrate outstanding thought leadership and business value.

Here are the 2018 winners.

Aetna

Safeguarding privileged access with behavioral analytics

■ Aetna is one of the nation's leading diversified healthcare benefits companies, serving more than 44 million people with information and resources to help them make informed healthcare decisions. With such a large potential attack surface, Aetna was concerned that its on-premises and cloud resources were vulnerable to insider threats and external account compromise — all of which could lead to privileged access abuse and data exfiltration. Moreover, the large volume of alerts sent to security teams was not risk ranked, which forced teams to randomly select which cases to remediate first. Aetna became the first organization in the healthcare sector to implement behavioral analytics for consumer authentication and access, and it now enables 80 percent of users to access their information with just their fingerprint.

Albertsons Companies

Evaluating security products, tools and services

■ Albertsons Companies, an American grocery company, needed a process to periodically review and realign controls, capabilities, services, and tools/technologies based on changing legal, regulatory, industry and business requirements. The company's information security department performed a bottom-up review of the tools, technologies and strategic partners required to support its existing and future requirements to ensure that investments remain leveraged and optimized. Its Tools Rationalization Project not only determined what technologies already existed in the Albertsons IT organization, but also what the digital transformation would bring. The effort identified several million dollars of savings over three years, codified strategic infosec technology partners and developed a three-year technology roadmap.

The Allstate Corp.

Leveraging security intelligence for improved supplier risk management

■ The Allstate Corp. is the nation's largest publicly held personal lines insurer, protecting 16 million households from uncertainties through auto, home, life and other insurance. As the threat landscape evolves and bad actors target Allstate's suppliers, Allstate proactively rebuilt its supplier security risk management process to safeguard all customer, agent and employee information. To improve the company's existing supplier security risk management function, the team rebuilt its pro-

CSO
FROM IDG

SVP/Publisher
Bob Bragdon

Executive Editor
Amy Bennett

Art Director
Terri Haas

Senior Editor
Michael Nadeau

Senior Writers
Steve Ragan, J.M. Porup

EVENTS

SVP/General Manager
Adam Dennison

Group Vice President
Anne McCrory

VP, Content Development & Strategy
Derek Hulitzky

IDG COMMUNICATIONS, INC.

President
Kumaran Ramanathan

U.S. President
Charles Lee

Founder
Patrick J. McGovern (1937-2014)

FOLLOW US
Twitter
Facebook
LinkedIn

492 Old Connecticut Path
PO Box 9208
Framingham, MA 01701

Phone: 508-872-0080

curement, privacy and information security process to incorporate industry best practices, frameworks and procedures. The effort reduced its supplier loss exposure by $7 million and reduced its supplier vulnerability communications from three days to less than one hour.

American Express Co.

Providing secure collaboration and enforcing cloud security policies

■ Cloud services are an integral part of American Express Co.'s IT strategy, especially as it moves to an agile development methodology. The company's information security department needed to support the business by providing a secure collaboration solution for thousands of developers and consistently enforcing global cloud security policies. By implementing Skyhigh Networks' cloud access security broker (CASB), American Express tangibly reduced its risk from shadow IT and securely enabled a cloud-based collaboration platform. The implementation of a CASB reduced risk exposure from the cloud, both from services currently in use as well as by blocking high-risk services as they pop up. Now, the information security team can keep up with and align itself with the company's agile technology strategy.

American Public Power Association

Assessing and improving physical security for critical infrastructure

■ The American Public Power Association (APPA) is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. While many security guidelines are available from the North American Electric Reliability Corp. (NERC) and other critical infrastructure sectors, public power utilities need a physical security guideline more focused on their needs. That's why the APPA created a comprehensive guideline designed to help the owners and operators of more than 2,000 community- and state-owned electric utilities better ensure the safety and security of their personnel, critical assets and information.

Arizona State University

Enhancing efficiency, accountability and collaboration

■ Arizona State University (ASU) is using Splunk to address multiple security use cases and increase the overall efficiency, accountability and collaboration among the university's IT operations. By centralizing key data into Splunk, distinct operational teams can access common data to answer critical business questions, enabling them to discover and remediate security threats faster and increasing overall business functions across critical university offices, including information security, PeopleSoft operations, system operations, development, the library, ASU police department's 911 call routing system, and admissions. Splunk has enabled ASU to reduce payroll and direct deposit fraud for the more than 14,600 people on its payroll, using sophisticated alerts to monitor all changes to direct deposits to safeguard ASU's $889 million annual payroll.

Bank of the Ozarks

Assessing the maturity of cybersecurity risk and controls

■ Headquartered in Little Rock, Ark., Bank of the Ozarks conducts banking operations through 252 offices across nine states and, based on asset size, has been recognized as a top performing bank in the United States for seven consecutive years. The bank nonetheless had no appropriate mechanism to assess its cyber-risk posture, nor did it have any appropriate mechanisms to assess the efficacy of its cybersecurity controls. To address that head on, it set out to establish a repeatable method to assess 149 critical security sub-controls and measure the inherent and residual risk to the organization. The new assessment procedures improved the maturity ratings of the vast majority of controls, all within the risk appetite defined by the board of directors.

Bechtel

Integrating processes, tools and knowledge

■ Construction and civil engineering company Bechtel needed a way to protect its critical corporate data. To do that, the company integrated a suite of processes, tools and knowledge that leverages the classification of information when it's created and ensures that all the information is appropriately protected. This has significantly reduced Bechtel's risk while allowing it to tailor and optimize work processes to its clients' requirements. From document creation to sharing, printing and storing information, Bechtel is now able to identify and restrict actions based on the sensitivity of the information, minimize potential issues with malicious access and better manage insider threats.

Bridgewater Associates LP

Building an enterprise risk management framework

■ Investment management firm Bridgewater Associates LP was looking for a tool to help it assess its risks and exposures. However, there was nothing on the market that matched the requirements of the company's security department. Therefore, Bridgewater developed the Risk Dashboard, which provides an interactive, single pane of glass showing real-time, multi-domain views into more than 500 different risk scenarios. This allows the company to quickly provide visualizations of enterprise risks for senior executives and security professionals, enabling highly informed risk-weighted decision-making. Now, Bridgewater can determine where to focus time and resources to most effectively protect the organization and the trust its clients place in the company.

Children's Mercy Kansas Hospital

Securing the hospital's environment and meeting regulatory requirements

■ Over the past decade, Children's Mercy Hospital has grown tremendously, but the hospital's information systems technology, particularly cybersecurity, has not kept pace. The hospital teamed up with PwC to develop a security roadmap and implement the new technology. As part of the project, the perimeter network environment was enhanced to improve the security posture of the hospital and increase internet speeds for users; threats were discovered and managed to identify vulnerabilities; access to information and the environment was protected to lock down access and implement the concept of least privilege; and processes were defined and improved to meet regulatory requirements and track change management. PwC's security service also allows the hospital to outsource security monitoring activities, enabling on-site resources to focus on other critical activities.

CLP Holdings Ltd.

Protecting critical infrastructure

■ CLP Holdings Ltd., an investor-owned power business based in Hong Kong, aims to protect its critical infrastructure from cybersecurity threats and ensure the security of its customers' energy supplies. To that end, the company is working with industry leaders and vendors around the world to develop software to expedite the advancement of critical infrastructure security. The overall objective within CLP's critical infrastructure is to provide a 24/7 security operations center to manage the security of its 66 sites across five regions. A key driver is the protection of the company's assets and the improved capability that comes with a standardized protection package across its entire fleet. Collaboration and partnerships with utilities and vendors are key to developing the technologies required to facilitate CLP's objectives.

Comcast Corp.

Quantifying the impact of cyber-risk

■ Comcast Corp.'s Cyber Value at Risk program, powered by the Bay Dynamics Risk Fabric platform, enables Comcast to continuously protect its most valued assets (data, systems and applications) by quantifying the impact of cyber-risk based on actual threat and vulnerability data in the environment and prioritizing mitigation actions based on those that reduce impact the most. The platform automatically delivers threat and vulnerability information to the stakeholders in the business responsible for mitigation and measures how much risk was reduced as a result of actions taken. With Risk Fabric's Cyber Value at Risk capability, Comcast's security team understands which threats and vulnerabilities need immediate action, and the platform uses the tools the company has already invested in so no money goes to waste. Risk Fabric enables the security team to direct its limited resources toward the most important problems.

Cook County Department of Homeland Security and Emergency Management

Enabling communities to fight cybercrime

■ Chicago's Cook County Department of Homeland Security and Emergency Management set out to provide a mechanism for a stronger, collaborative front against malware, DDoS (distributed denial of service) attacks, ransomware and other methods of cybercrime for municipalities and communities with limited resources. The department needed to create an effective threat notification service that formats alerts that are actionable for security specialists and easily understandable for city and county analysts. The solution: the Cook County Cyber Threat Intelligence Grid (CCCTIG), which integrates with existing infrastructure and allows sharing with external entities in a secure manner. The CCCTIG provides a security solution for communities that cannot afford the cost of cybersecurity solutions, providing an enhanced level of automation.

Cox Automotive

Adopting modern practices for improved cloud security

■ Cox Automotive is transforming the way the world buys, sells and owns cars with digital marketing, financial, retail and wholesale solutions across the global automotive ecosystem. As the company continues to move internally developed internet-facing applications — like Autotrader.com and KBB.com — into cloud environments, it needed a better solution to manage how to implement, monitor and audit controls across security, architecture and operations, ultimately to meet its compliance, legal and regulatory requirements. The company's new cloud monitoring technologies not only discovered hundreds of suboptimal configurations, privileged access and vulnerabilities, but also enabled fresh visibility to prioritize and remediate findings.

Cleveland Metropolitan School District

Leveraging awareness to reduce the cost of phishing attacks

■ The Cleveland Metropolitan School District is the second largest school district in Ohio, serving students across 82 square miles with a rigorous curriculum that considers the individual learning styles, program preferences and academic capabilities of each student. After 74 employees in the district received a phishing email and provided their payroll usernames and passwords — resulting in a substantial financial cost — the district realized that its 7,500 staff and 40,000 students needed to be more knowledgeable cyber-citizens. The district implemented a security awareness program that dramatically reduces its costs related to phishing attacks.

Delta Dental Plans Association

Enhancing the security of the Delta Dental brand

■ Delta Dental Plans Association (DDPA) wanted to create a set of security standards across its 39 Delta Dental member companies to reduce the overall risk to the Delta Dental brand. To accomplish that goal, DDPA created a standard control set across member companies, leveraging economies of scale to allow member companies to save money on security. The new security program has also allowed for increased collaboration across the member companies, provided a way for the system to come together to answer national requests for proposals, and enhanced the overall security behind the Delta Dental brand. By leveraging a collective process to purchase on behalf of the system, DDPA has enabled member organizations to save anywhere from 25 percent to more than 50 percent on the cost of security products.

Ellie Mae

Identifying indicators of compromise

■ Ellie Mae, a cloud-based platform provider for the mortgage finance industry, has developed a program that identifies indicators of compromise (IOCs) as early as possible; provides the best threat data feeds and integrates them with Ellie Mae's advanced security tools; and generates strategic cybersecurity threat intelligence that provides insights on adversaries' motives and tactics. The Cybersecurity Threat Intelligence (CTI) program exposes hackers' reconnaissance, intercepts them, and gives Ellie Mae the ability to detect and respond to attacks faster, enabling the correlation between attack sources, methods and techniques. CTI has increased the security organization's productivity, as the threat intelligence has greatly increased the number of threats the security team can identify, assess, contain and mitigate.

Fannie Mae

Journey to DevSecOps

■ Fannie Mae partners with lenders to create housing opportunities for families across the country and helps make the 30-year fixed-rate mortgage and affordable rental housing possible for millions of Americans. To support its mission, Fannie Mae must support robust security practices throughout the organization. For years, Fannie Mae has aimed to 1) conduct cybersecurity assessments earlier in the development lifecycle, and 2) engage business partners in the review and mitigation of cybersecurity risks. Through DevSecOps, Fannie Mae has now reached that goal: Stakeholders from development, operations and cybersecurity can now monitor, analyze, test, and proactively determine and fix vulnerabilities earlier in the development lifecycle.

Finicity

Leveraging culture to achieve rapid SOC compliance

■ Founded in 1999, Finicity is in the business of providing personal financial management and consumer financial wellness. In March 2016, a large consumer financial organization approached Finicity to participate in Series B funding for expansion, but Finicity would have to achieve Service Organization Control (SOC) compliance within six months and successfully adopt security controls to pass scrutiny by multiple financial institutions and security organizations. The Finicity team achieved its goal by rapidly adopting a culture of mission-critical security and implementing state-of-the-art infrastructure — all of which now withstands the scrutiny of several top 10 financial institutions.

Finning International

Managing change to improve cybersecurity awareness

■ In business since 1933, and now employing more than 12,000 people around the world, Finning is the world's largest dealer of Caterpillar heavy-industry equipment. To improve its cybersecurity posture, Finning's IT security team implemented a global cybersecurity awareness campaign designed to 1) enable employees to better identify and respond to potential cybersecurity incidents, and 2) elevate a cybersecurity culture so it's as routine as the company's already-pervasive health and safety environment. It has now rolled out this program in multiple languages and geographies, which has been a valuable lesson in managing change.

GE Aviation

Minimizing insider threats with machine learning

■ GE Aviation is a global provider of jet and turboprop engines, components, integrated digital, avionics, electrical power and mechanical systems for commercial, military, business and general aviation aircraft. Since GE Aviation leverages cutting-edge designs, light and strong materials, and advanced manufacturing processes, protecting intellectual property is a top priority for the business. To improve data loss prevention, the GE Aviation data security team created an insider threat tool leveraging an indicator correlation methodology that locates users who produce critical risk-based alerts.

Genpact

Improving incident response

■ With 78,000 employees in 20 countries, Genpact is a global professional services firm that manages digitally enabled intelligent operations for Fortune Global 500 companies. Recognizing that sophisticated threat actors pose significant risks, the organization developed a plan to enhance its incident response capabilities. The company's modernized security intelligence leverages user behavior analytics technology for insights into risky user behavior and potentially compromised accounts, and enhances investigation and forensics capabilities. It has also improved detection and response times with automation.

HBO Latin America

Making incident identification and response more efficient

■ HBO Latin America was looking for an effective way to analyze network traffic without creating additional strain on the IT organization. By implementing Vectra and integrating it with Splunk and Carbon Black, HBO Latin America was able to leverage artificial intelligence to automate the analysis of the immense volume of security events. Alerting the team to only critical or immediate threats enabled it to make better use of its time. After Vectra was introduced and the integration with other solutions was completed, there was an immediate decrease in total volume of security alerts and an increase in the accuracy of those alerts.

Health Management Systems

Creating a secure cloud infrastructure

■ Health Management Systems, a provider of cost containment software to the U.S. healthcare market, wanted to create an environment that could support highly sensitive data and meet its high security standards while complying with government and commercial compliance frameworks. The business objective was to support new product innovation that could be hosted in the Microsoft Azure cloud environment. It was imperative that HMS be considered a company that looks for new and efficient ways to meet market demand by leveraging a cloud-first adoption strategy. It was also imperative that the company didn't abandon its existing technology base and leave customers stranded on legacy platforms. To meet these objectives, the HMS security and IT Infrastructure organizations created a secure cloud infrastructure within the Microsoft Azure environment that supports authentication, authorization, auditing, monitoring, network control and malware protection.

Hindustan Petroleum Corporation Ltd.

Implementing an anti-APT solution

■ To protect its critical information infrastructure, Hindustan Petroleum Corporation Ltd. (HPCL) had previously implemented signature-based security solutions, such as next-generation firewalls, intrusion detection/prevention system solutions, and web and email gateways at the data centers hosting critical applications. Then, to mitigate targeted and unknown zero-day attacks, HPCL decided to implement an anti-advanced persistent threat (anti-APT) product. After implementing anti-APT, the visibility of the attack vectors was improved and no other malware or ransomware attacks were reported within HPCL's environment. In addition, by integrating all the security solutions and enabling them to share threat intelligence, most of the threat vectors have been mitigated. On average, five to 10 unique attack-like scenarios per month, via email and web channels, are now being reported and mitigated by the anti-APT solution.

Horizon Blue Cross Blue Shield Of NJ

Building an early vulnerability detection system

■ To be more proactive about responding to the millions of attempts to breach its systems every day, Horizon Blue Cross Blue Shield of NJ built the Early Vulnerability Detection System (EVDS), a new system that identifies vulnerabilities throughout a project lifecycle and facilitates development of multiple levels of defenses within the organization's applications. The EVDS is a combination of people, processes and technology that fully adjusts to the diverse nature of current technologies. Security recommendations are delivered via the basic elements of a standard project: business requirements, architecture design and test cases. The EVDS has already identified and remediated more than 700 critical vulnerabilities that would have resulted in catastrophic breaches. Additionally, 100 percent of newly discovered vulnerabilities that were tracked as application defects were remediated before the application was released into production.

Infosys Ltd.

Leveraging analytics to detect and protect against insider threats

Headquartered in Bengaluru, India, Infosys provides technology services and consulting to large enterprises. Since many of its 250,000 employees have access to confidential customer information, Infosys was concerned about privacy violation liabilities. As such, the company wanted the ability to detect and protect against insider threats as well as external attacks that use compromised insider credentials. To that end, Infosys deployed a security analytics platform from Gurucul to apply machine learning algorithms to user activity to discover privileged access events and detect anomalies in user and entity behavior. The project enabled Infosys to increase anomaly detection by 33 percent and reduce open security investigation cases by 56 percent through a radical decrease in false positives.

Innogy SE

Transforming the security organization

Serving 23 million customers with 40,000 employees across 16 European countries, Innogy SE is addressing the new requirements of a decarbonized, decentralized and digital energy world. As conventional power plants shut down due to poor economic performance, profits shrink and cost-saving measures become critical. For Innogy SE, this meant reinventing the organization's approach to energy, and for the Innogy SE security team, it meant reducing costs by 25 percent while maintaining the highest security standards for the organization moving forward.

Jackson Health Systems

Consolidating key technologies

While the IT security department at nonprofit academic medical system Jackson Health Systems (JHS) had been very successful procuring and deploying many key technologies, lack of integration meant that the team was relying and focusing on just one or two solutions and ignoring the rest. One of the key goals was to make the best use of the security investments the IT security team had made as well as make better use of the intelligence gleaned from the data captured by disparate systems. To accomplish those goals, the JHS IT security department consolidated the key technologies it had deployed over the past two years into a robust security operations center that would enable the team to identify, mitigate and stay one step ahead of cyberthreats.

Kimberly-Clark Corp.

Creating a proactive, risk-aware culture

With 42,000 employees worldwide, Kimberly-Clark Corp. sells leading brands in more than 175 countries. To better assess and control threats to critical information systems and reduce its risk profile, the organization implemented a corporatewide risk management framework. Designed to drive a proactive, risk-aware culture, this new framework includes an automated tool to increase efficiency in managing risk, enhance risk communications and boost agility in risk response.

Lennar

Creating a physical and information security program

■ In 2015, when Juan Gomez-Sanchez joined home construction company Lennar as its first chief security officer, he was tasked with creating and implementing a physical and information security program to support seven lines of business, more than 8,000 associates and 900 locations operating in 17 U.S. states and 44 markets. Gomez-Sanchez and his team built Lennar's security program from the ground up with a holistic and business-centric approach to risk management, creating an environment of accountability and transparency. The team also implemented a security operations center that deployed numerous technologies, refreshed older technical controls and established a governance model represented by all lines of business. Lennar's security program has made the entire organization more agile and prepared to react to challenges.

Lifespan

Recruiting and retaining security talent

■ As part of its ongoing security program, the chief information security officer of Lifespan, Rhode Island's first health system, designed and implemented the Golden Gauntlet program in response to the constant struggle to recruit, hire, motivate and retain competent information security professionals in a hot market. This program has effectively addressed "wrong-fit" candidates and hires, and created a high-performance, low-attrition team that is now detecting 94 percent more incidents. One measurable business result of the Golden Gauntlet program has been a reduction in recruitment fees. Since the start of the Golden Gauntlet program, Lifespan has reduced the information security team's annual recruitment fees by 90 percent, primarily by selecting the right people the first time. And because Lifespan has the right talent, security incident detection has increased from 50 to 750 incidents per month.

Merit Network

Promoting security careers

■ Founded in 1966, and governed by Michigan's 12 public universities, Merit Network is a nonprofit, member-owned organization that operates America's longest running regional research and education network. As in countless geographies around the world, Michigan's business community faces cybersecurity as well as economic and talent development challenges. To address this, the Governor's High School Cyber Challenge was created to spark cybersecurity interest among high school students and inform them of current talent shortages in the United States. Designed to challenge students' skills across computer science, information technology and cybersecurity, a two-round competition culminated at the governor's annual North American International Cyber Summit, which spanned 13 time zones, six countries and 12 states.

Micron Technology Inc.

Implementing big data security and access controls

■ As one of the most prolific patent holders in the world, intellectual property is the foundation of Micron Technology Inc.'s business. Adequately protecting that data while enabling the business is critical to ongoing success. So, the company embarked on a project to develop an access management framework for the new Micron global data warehouse that would take advantage of the game-changing power that big data and advanced analytics techniques can offer. Micron also wanted to maintain principles of least privilege in the governance of its valuable data and reduce friction on access controls to enable rapid results. Successfully implementing big data security and access controls enabled Micron to effectively access and utilize its valuable data, improve its manufacturing operations, and maintain its position as one of the world's leading memory and storage manufacturers, all while protecting its valuable intellectual property.

NorthShore University HealthSystem

Improving the evaluation and onboarding of medical devices

■ NorthShore University HealthSystem's health information technology and clinical engineering departments collaborated to improve the security evaluation and onboarding process of medical devices. The organization created a detailed process and assessment form that allows teams to understand risks before purchasing and installing medical devices. This work was done to identify risks and mitigation opportunities, inform operational stakeholders and pressure vendors to comply with security controls. As a result, NorthShore has been able to identify 400 networked medical devices that require special attention related to patch management. And the organization has raised awareness of the issues with its operational counterparts in clinical engineering, purchasing and operations.

Polaris Alpha

Stonewalling ransomware before it hits production assets

■ With research, exploration and problem solving, Polaris Alpha provides engineering and tools designed to protect the warfighter and allied communities. Like many organizations targeted by ransomware, Polaris Alpha knows it can face significant mitigation and recovery costs not only in terms of data and productivity loss, but also fixes and possible regulatory penalties. With that in mind, the organization began to apply the concept of honeypots to delay and detect a ransomware infection. The STONEWALL project uses deception technology to create a ransomware-defendable network that chokes and slows down a threat, alerting security teams before the ransomware attacks production assets.

Premise Health

Establishing a security operations automation and orchestration strategy

■ Premise Health manages more than 500 worksite health and wellness centers across the U.S., serving more than 200 of the nation's premier corporations, many of them among the Fortune 1000. Previously, Premise's component firms outsourced the functions of their security operations centers (SOC). However, Premise decided that it had to establish an in-house SOC with expanded processes, people and technology, while providing strong security for the combined firm's infrastructure and data and avoiding gaps in security monitoring. To that end, Joey Johnson, the company's chief information security officer, devised a security operations automation and orchestration strategy that enabled Premise to establish previously elusive metrics measuring both SOC and IT effectiveness, and demonstrating ROI for the decision to build vs. outsource. Additionally, the project helped the IT infrastructure team increase security through improved patching discipline and antivirus update practices.

Prudential Financial

Reinforcing security culture

Prudential Financial's global security department developed a mobile app for all employees that provides safety tips and the latest updates on events that could impact them. The project was designed to reinforce a security culture within Prudential. This project is the second version of the mobile app, intended to improve the digital experience by enhancing its look, usability, functionality and navigation. The tool is used as one of the mechanisms to share security tips, alerts and advisories. The Global Security Mobile application has allowed Prudential employees to receive real-time alerts during company and outside emergencies. The new version of the application enhances the overall employee experience by providing instant access to information on the go, as well as changing how employees communicate and interact with the global security department.

Rainforest Alliance

Creating training materials for security awareness

The Rainforest Alliance, a global nonprofit organization that works to conserve biodiversity, protect the environment and ensure sustainable livelihoods, has started creating training materials to educate staff and other users around the world regarding the need for security awareness and IT controls to prevent data breaches. In the past, the Rainforest Alliance had conducted a series of IT webinars to address the security concerns of the organization. However, these webinars were not well attended for various reasons. So, the organization decided to create multiple short animated videos to keep viewers' attention as well as educate them regarding the need for complex passwords and how to recognize a phishing attack, for example. Since starting the program, the Rainforest Alliance has increased the participation rate of employees and expanded its target audience by more than 87 percent.

State of Michigan, Department of Technology, Management and Budget

Creating an all-volunteer force of cyber-defenders

With the realization that small and midsize businesses and local governments are likely facing the same cyberthreats, the state of Michigan created the Michigan Cyber Civilian Corps (MiC3), an all-volunteer force of cyber-defenders to supplement its publically available resources, such as the Michigan National Guard and the Michigan state police. Michigan is the only state with an all-volunteer cyber corps and is routinely contacted for guidance from other states. The MiC3 will help the state respond to cyber-incidents during a governor-declared state of emergency. The new team of volunteers will work with existing state IT staff and resources to create a broader network of cyber-responders. As it continues to test and assess the effectiveness of the MiC3, Michigan intends to continue sharing the details of the program with other states.

Teachers Insurance and Annuity Association

Implementing an automated certificate management and security system

The Teachers Insurance and Annuity Association (TIAA) needed an automated, companywide certificate management and security system to reduce the time and resources required to provision certificates. The organization launched an aggressive project in May 2016 to meet upcoming SHA-1 deadlines that delivered far more results than expected. In addition to dramatic reductions in certificate overhead and delivery times, TIAA also reduced outages and added several new integrations and tools that measurably improved security. The organization also improved partnerships with internal and external stakeholders. The entire project was delivered ahead of schedule and resulted in substantial, measurable savings to TIAA's bottom line. The automated approach reduced certificate delivery time from three days to seconds. Before the project implementation, the cost for 1,000 certificates was $60,000; after implementation, the cost for $1,000 certificates was $120.

The Clorox Co.

Implementing an advanced threat management program

■ Following the National Institute of Standards and Technology (NIST) framework, The Clorox Co.'s IT security department developed an advanced threat management program to quickly and efficiently detect and defend against advanced threats within the company's environment. A threat management process supported by next-generation security products is part of a program that provides IT security with better visibility into potential threats and creates a solid foundation to detect and defend against these threats. These actions will help reduce business risk, protect Clorox assets and preserve its reputation. Clorox detected hundreds of suspicious events and malicious files within the first 30 days after the project was deployed, reducing the risk to the network and IT environment.

The Home Depot

Gaining visibility into the networks of acquired companies

■ After a security breach, The Home Depot's information security leadership team increased its proactive strategy for addressing cyberthreats. The company's growth strategy involves actively acquiring other companies, and a key priority is to establish visibility into the networks of its acquisitions to understand vulnerabilities that may exist. Beyond gaining this initial visibility, Home Depot needed a reliable way to detect any new threats inside the network. This challenge caused Home Depot's information security team to proactively work with the subsidiary teams to assess and elevate security controls where needed. This approach helps the company gain the needed visibility to quickly detect cyberattackers. The project reduced false alarms and greatly increased the productivity of the security operations staff.

Tift Regional Health System

Improving infrastructure security

■ Tift Regional Health System (TRHS) is a growing not-for-profit hospital system serving 12 counties in South Central Georgia, offering more than 135 physicians with expertise across 30 specialties. Like other healthcare organizations facing growing security threats and gaps in endpoint security, TRHS needed a plan to enhance its existing IT security infrastructure through improved virus protection, network port protection and training. TRHS not only secured a go-forward plan from the board, but successfully implemented the plan to achieve measurable results.

United Nations Development Programme

Performing real-time incident detection

■ The United Nations Development Programme (UNDP) cyber-incident response team significantly upgraded its capabilities to become an international model of best practice, in part by providing cybersecurity assistance to developing nations. First, the UNDP developed a system that pinpoints potential compromises by comparing known malware indications with the security traffic feeds from UNDP's 177 offices. Second, it developed a threat intelligence and website scanning capability to identify potential risks to the organization. Third, the organization improved readiness by developing in-house exercises and participating in capture-the-flag competitions. Finally, the cybersecurity team sponsors annual international conferences to train IT personnel from developing nations. The organization can now perform real-time incident detection by matching network traffic from its global network of offices against known indications of compromise based on threat intelligence.

University of California

Reducing the risk of cyberattacks

■ Following a significant cyberattack, the University of California undertook a fundamentally different approach to managing its cyber-risk program based on the five core pillars of cyber-risk management: governance, risk management, modernizing technology, common solutions and cultural change. These pillars supported all aspects of cyber-risk management, and were used to reduce the risk of cyberattacks across 10 campuses and five health systems. As a result, the ability to detect and respond to threats across all campuses and health systems went from days and weeks to less than a few hours. Cybersecurity training was mandated, with nearly 90 percent compliance in the first year and 95 percent compliance in the second year. In addition, a state-of-the-art information security policy was developed, and notifications due to breaches have dropped significantly.

University of Pennsylvania

Automating handling of Tier 1 security events

■ Due to its unique mission and user base, the University of Pennsylvania (Penn) experiences as many as 10,000 Tier 1 information security events each year. Penn has dramatically reduced its cybersecurity risk by automating the handling of 86 percent of its security operations center (SOC) Tier 1 security events, saving hundreds of thousands of dollars per year. The automation of these important, but lower risk, events allowed the Penn SOC to quickly and effectively address more costly, high-risk events. Minimizing Tier 1 staffing allowed the organization to retain experienced Tier 2 and Tier 3 analysts, resulting in further improvements in detection, prevention and response. The Penn Office of Information Security program has been able to defer the need for SOC Tier 1 staff, interns or other, similar junior analysts. Because increasing head count and space both present significant financial and political challenges in the current university IT environment, this has been an important outcome.

State of Missouri, Office of Administration

Delivering targeted security lessons

■ Covering more than 70,000 square miles, the state of Missouri is home to nearly 6 million people. To elevate the ability of the Office of Administration's (OCS) 40,000 employees to address security threats beyond simply consuming passive annual training, OCS began deploying targeted, focused and interactive lessons each month. Since inception of this new program, nearly 1 million individual lessons have been delivered, tracked and gamified to the individual — and participation and results have been graded and shared throughout state government.

Xerox: Xerox Enterprise Cyber Threat Management Portal

Providing transparency to stakeholders

■ Xerox is an $11 billion technology company committed to accelerating business, whether paper or digital. Its 39,000 employees are focused on automating, personalizing, packaging, analyzing and securing information for small and midsize businesses, large enterprises, governments, graphic communications providers and the partners that serve them. Like most organizations, Xerox experiences increasing demand from concerned customers, executives, partners and board members to demonstrate cyberthreat awareness and the ability to respond in real time. To meet this challenge, it created the Xerox Enterprise Cyber Threat Management Portal — a custom-designed solution that provides intelligence-driven, cyberthreat readiness and situational-response task workflow management. The system responds in real time to disseminate bulletins from the CISO's organization to a defense-in-depth matrix "playbook" of global IT and security operations teams and business focal points.

Xerox : Xerox's Global Security Services

Reimagining security to change team culture

■ To adapt to evolving markets and drive innovation for better solutions, it became critical for Xerox's security services organization to operate in lockstep with the company's vision. The organization successfully reimagined Xerox's Global Security Services organization and successfully cultivated changes in team culture to improve results. ♦