CSO
FROM IDG

Spring 2017

CSO50 AWARDS 2017

A step ahead

This year's CSO50 winners are designing security to stay in front of modern threats

HONOREE: How IACI's "neighborhood watch" aims to change the information sharing landscape

CSO 50 AWARDS 2017

Now, more than ever, security leaders must collaborate

IF THERE'S BUT ONE thing that we can take from the past 12 months, it's that security should never be taken for granted, despite every belief to the contrary. Research tells us that collaboration around security has been in decline since 2010, but now, more than ever, CSOs need to lean on each other to address the array of risks that your businesses face.

What's getting in the way of good collaboration? Two things: fear and technology. The technological hurdles you must overcome can be massive: incompatible sharing platforms, lack of standards, the actual process of how, and with whom, you share. So instead of having effective one-to-many information sharing, we continue to fall back to one-to-one and one-to-few models. Of course, that's what makes peer events like CSO50 so important.

A number of events happened over the past 12 months that every business should take note of because they are indicative of deeper challenges that need to be understood and addressed:

WikiLeaks Part 1: the information thefts around the 2016 U.S. Presidential campaign. The lesson: anyone can be breached, but good cyber hygiene would have gone a long way to reducing the victim's risks.

One company name explains why senior management and Boards of Directors should care about security for the foreseeable future: Yahoo. Following on the revelation that a data breach years earlier had exposed over one billion records, Verizon wrote-down their acquisition cost of Yahoo by $350 million (IMHO, a drop in the bucket compared to what the actual cost of that breach will cost them). The lesson: This was a hard, bottom-line impact to a major business acquisition due to senior management's decision to ignore good security (reach out and I'll fill you in).

WikiLeaks Part II: the CIA and Vault 7. The impact has the potential to be a massive hit to U.S. intelligence-gathering efforts due to what appears to be an insider event. The lesson: no organization is safe as long as there are humans involved.

The massive DDOS attacks against Dyn and Brian Krebs, which exposed the threat posed by unsecured IoT (internet of things) devices that have been proliferating for years. The lesson: security needs to be built into everything.

I hope that we will see improvements on all these and hope that senior leadership will continue to appreciate the importance of good security. I hope for a lot of things, but as a former colleague liked to say, "hope is for children."

–Bob Bragdon, Publisher
bbragdon@cxo.com

CSO50 winners are out in front

IN REVIEWING THIS year's pool of CSO50 award applicants, it was clear just how much security has evolved and matured. Projects submitted this year ranged from awareness initiatives, to threat analytics, to collaborative security, to identifying vulnerabilities and specific insider threats. These are just a few examples of the individual missions of the award-winning projects we will honor here at CSO50 this week. But as diverse as the projects may be, they have common threads. Chief among them is the aim to stay one step ahead of the threats that organizations face today.

For many years, as the role of the CSO was expanding, security often played an all-too frustrating game of catch up. Industrious criminals were often out in front of security strategy and finding new ways to siphon sensitive data and expose a company's private assets for their own personal, illegal gain. But this year's crop of CSO50 winners prove that good defense is not simply a case of catch as catch can in the enterprise. As our conference theme indicates, these award-winning projects aim to align proactive security with modern threats.

Ransomware, lack of user awareness, internet of things vulnerabilities and the wide-reaching implications for them are all hot topics we are following now at CSOonline. As you read through this supplement, note how many of our award-winners are on top of, and even in front of, these problems today because of forward-thinking security projects within their organizations. We hope learning more about this year's projects, and the collaborative time you will spend with industry peers, will leave you feeling inspired to head back and take a fresh look at what your organization can be doing now to modernize your security infrastructure and posture your security strategy to match today's threat landscape.

Congratulations to all of this year's CSO50 honorees.

–Joan Goodchild, Editor in Chief, CSOonline.com

CSO

Publisher
Bob Bragdon

Editor
Joan Goodchild

Art Director
Steve Traynor

Managing Editor, Production
Bob Rawson

Contributors
Stacey Collett

Editorial Administrator
Pat Josefek

IDG Communications, Inc.

Founder
Patrick J. McGovern

CEO
Michael Friedenberg

Editorial/Advertising/ Business Offices
492 Old Connecticut Path
P.O. Box 9208, Framingham, MA
01701-9208

Main phone number
508 872-0080

BPA WORLDWIDE

CSO 50 AWARDS HONOREE 2017

International Association of Certified ISAOs

Changing the information sharing landscape BY STACY COLLETT

Michael Echols, IACI CEO and executive director

THE FEDERAL government for years has advocated that cyber-threat information-sharing is the key to faster identification and remediation of attacks. The challenge was to make once-taboo information sharing more inviting to the private sector, and to educate organizations about its benefits.

IACI, an international non-profit association that fosters information sharing and collaboration among certified information sharing and analysis organizations (ISAOs), was launched in June 2016 to accomplish just that — to create a nationwide network of cybersecurity "neighborhood watch" groups that will fundamentally change the information sharing landscape.

No other organization in the nation coordinates cross-sector analysis through direct work with communities of interest and links them to partners to enhance cyber intelligence, IACI leaders say. IACI partnered with the Department of Homeland Security and the FBI to create an anonymized information sharing mechanism between the private sector and the government.

"The idea [for the initiative] was that, the government can't protect you — it's trying to protect itself, and one of the greatest ways to reduce risk is through information sharing," says IACI CEO and executive director Michael Echols, a former DHS senior cybersecurity executive. "If you're in a trusted group with other companies, if something happens to you, the same thing shouldn't happen to them."

In just four months, IACI helped establish industry specific information sharing groups for credit unions, maritime and port security, critical manufacturing, air and space organizations, cyber response entities and national rural health. In December, a national election system ISAO was launched, plus commitments from business and university groups in Chicago and Southern California.

The national credit union ISAO quickly became the largest information sharing group with almost 50 member organizations, even though credit unions are part of the financial services industry, which bears the gold standard for information sharing.

"Credit unions are really unique" compared to the rest of financial services, says Gene Fredriksen, executive director of the national credit union ISAO. "They're not for profit and have relatively small staffs. Large banks may have hundreds of security analysts, while credit unions might have one part-time analyst. That means everything that they need also needs to be very actionable." Instead of receiving 1,000 security alerts a day, "they need two alerts a day that are very applicable to credit unions," he adds.

The ISAO also wants to accelerate the cyber-threat maturity of credit unions. "They might not have six weeks to research and write a document" when they discover a vulnerability. "But if they can find what their peers have written and do it in six days, you've accelerated their maturity," Fredriksen says.

Some of the IACI's biggest challenges are basic awareness and helping organizations understand how they can reduce their risk of cyber threats by being part of a sharing organization.

"Just sharing for [the purpose of] national security is not enough for most businesses," Echols says. They need to understand the business benefits, too. "Previously, the issue was that it was a liability to actually share information," Echols says. "The government is trying to flip that, but the private sector has to take the lead here in changing these dynamics."

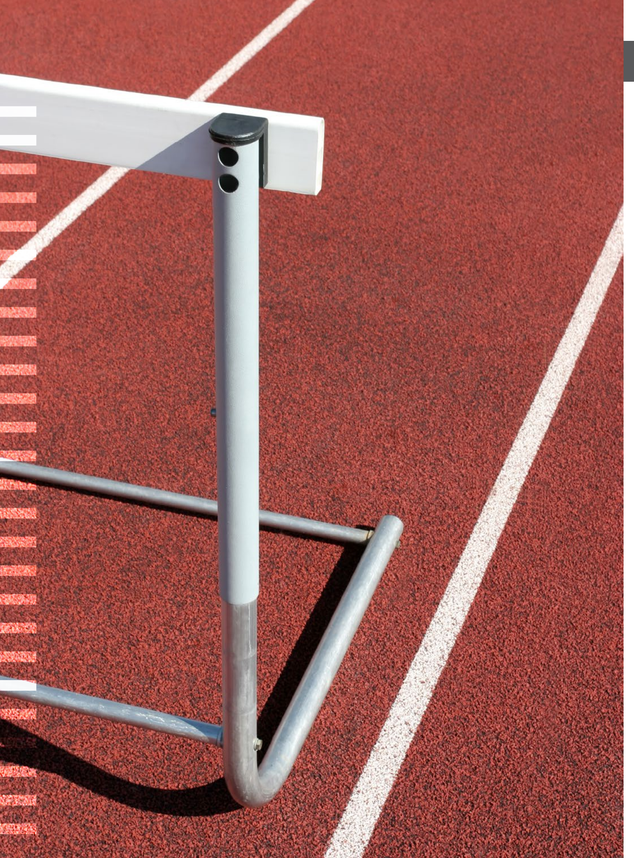
Another major business benefit, Echols says, is that regulators are now looking at organizations' cybersecurity practices. For instance, he points to the FDA's recent recommendations for medical device makers indicating that if they identify a vulnerability, fix it within 30 days and then share information with an ISAO, then the FDA won't enforce compliance

PHOTO BY NOAH WILLMAN

of its own reporting requirements. "There's a clear path — you can see where we're going," Echols says.

In a short time, IACI has created a model of inclusion to let all entities, including small and medium-sized businesses, take part in cyber intelligence activities designed to expand cyber resilience.

IACI was launched by the Global Institute for Cyber Security + Research, Defense Industrial Base Information Sharing and Analysis Center, and Webster University. ■



A step ahead *of the* threats

The **CSO50** awards honor innovative security projects that demonstrate thought leadership and outstanding business value BY STACY COLLETT

Voya Financial

Proof of information security

■ The financial services industry's information security practices are under tight scrutiny by auditors, regulators, clients and vendors. Voya Financial faced increasing challenges to provide security information and evidence to these groups in an efficient manner while maintaining quality and consistency.

Voya implemented a tool called GEAR (Guidance for Evidence, Artifacts and Responses), a highly searchable database for internal auditors that provides accurate and current information, and gives Voya an end-to-end view of its control posture and compliance with policy.

Prior efforts to create the database focused primarily on the questions that auditors might ask. Different auditors could word the question differently, resulting in individualized responses. The new approach focuses on the answers — taking the position that controls are what they are. If Voya understands the control being asked about, it can supply the answer quickly and easily.

Project leaders say the tool has sparked a significant culture change within the audit response team as it moves away from "reacting to audits" to proactively reporting on the effectiveness of controls.

Viewpost

Cagey — Financial Crime Insight Mapping

■ Knowing good customers from cybercriminals is key for any financial institution. The security, fraud and financial crimes teams at B2B payment platform Viewpost developed software called Cagey that analyzes all customers based on their risk, financial crime status and relationships with other companies. The software then displays who may be someone they want to watch, take off the platform, or allow to continue transacting business.

The Viewpost team created a unified financial crime platform that graphically displays all customers and their risk score on the platform, their relationship with other vendors and buyers, their association with bad customers tied with improper transactions, their association with fraudsters, and those who have been taken off the platform. All cyber, fraud, anti-money laundering, and other company risk data is pulled together, analyzed and displayed in color format so that the company can predict who is at risk of committing a financial crime or who is already a fraudster.

As a result, the graphical display map has cut down fraud and is beating banks in reporting this information by two to three days.

USAA

Identity and Access Management Lifecycle Management

■ At insurance company USAA, many events over a worker's career can affect the type and level of access they have to company information — a promotion, termination or a move to another department. These manual changes often took five days to implement, not to mention the time needed to ensure that these changes wouldn't impact customer service.

The Identity and Access Management (IAM) Lifecycle Management program established automated processes to create new worker accounts and provide basic accesses immediately, monitor and react to transfers that occur within the organization, and ensure that terminated worker accounts are quickly closed.

USAA workers are now productive within minutes of onboarding, and workers do not retain privileged accesses when they transfer from one position to another.

When a worker is terminated, the system automatically removes privileged accesses in near real-time.

What was a five-day, manual IAM process has been reduced to less than 15 minutes.

United Nations International Computing Centre

UNICC Continuous Security Improvement Suite

■ In 2013, the United Nations

acknowledged that information technology has helped advance its ability to bring peace, prosperity and dignity to the world. The next challenge was to explore how the United Nations family could protect those gains and create a more secure cyber environment.

The UNICC Continuous Security Improvement Suite project began in late 2014 to deliver on those goals. The project has four components — One ICTbox is a rapidly deployable modular infrastructure for UN field offices with built-in security controls. Common Secure is a cyber security information-sharing/threat analysis community network. Common Connect allows UN agencies to collaborate and share information assets. Information Security Governance and Operations offers IS advisory support and operational solutions for smaller UN agencies to implement and manage ISMS standards and processes.

UNICC's information security solutions have enabled partner agencies to share information security resources and has reduced the cost of building solutions from scratch for all UN agencies.

United Airlines

Bug Bounty Program

■ United Airlines manages over 93 million Mileage Plus accounts containing hundreds of millions of miles. Customers' miles are valuable not only to them, but also to malicious outsiders intent on stealing and converting the miles to other products, such as travel or consumer electronic equipment.

To stop the cyber thieves, United invited the world's most creative and skilled white hat hackers to its Bug Bounty program, which offers compensation in the form of miles to those who find and report security bugs on United.com and other web properties before the bad guys do. The program has proven to be a rapid method to identify highly difficult-to-discover code defects, and for a modest cost to United.

The program's success is measured more by cost avoidance as opposed to ROI, according to United. With the average cost of a data breach at about $154 per record lost, United says that creative approaches such as the Bug Bounty program are required to manage risk and reduce potential costs, while providing enhanced protections for United customers.

TransUnion

TransUnion Enterprise Security Ratings Platform

■ As a service provider to many financial institutions, insurance companies, health care organizations and government agencies, TransUnion's information security program is constantly being evaluated.

To meet customers' stringent requirements, TransUnion launched its Enterprise Security Ratings Platform (SRP), which gathers terabytes of data from security sensors around the world and provides insight to indicators of compromise, infected machines, improper configuration, poor security hygiene and harmful user behavior. The data is analyzed to determine the severity, frequency and duration of incidents and then mapped to known networks, resulting in an overall security rating for each selected organization.

The ratings provide continous insight into each organization's security posture and is used in TransUnion's third-party security program, self-assessment exercises, security benchmarking, and mergers and acquisition activities.

The platform has resulted in improved security, transparency and efficiency. SRP enables TransUnion to monitor as many as 10-times more service providers on a continuous basis. SRP generates benchmarking reports that compare TransUnion's security posture to its competitors, and it improves efficiency without increasing headcount.

The Nature Conservancy

Security Analysis Architecture Project

■ Timely knowledge of cyber attacks on The Nature Conservancy (TNC) are the cornerstone of risk operations. Without accurate knowledge of attack profiles, many tasks become impossible, such as managing risk, determining what to secure and identifying layered controls.

Rather than relying on instinct, TNC opted for data-driven decisions. Its Technology and Information Services team developed a comprehensive security analysis architecture. The solution contains two components — a sensor infrastructure that is embedded at field offices, and a centrally managed log/visualization infrastructure, which serves as the focusing system for aggregation, parsing, visualization and analysis.

Developing such a sophisticated system is financially challenging for most non-profits. TNC used white box servers, repurposed consumer gaming devices as sensors, and leveraged open source or free tools to accomplish this task.

Sensors have been deployed to field offices across the U.S. These sensors captured approximately 65,000 unique indica-

tors that will be used to create concise executive level reports for the first time, which will help them measure risk exposure and drive its cybersecurity direction.

The Mitre Corporation

ATT&CK

■ The key to a successful cyber defense is understanding an attacker's tactics and techniques. MITRE has developed an adversary playbook called ATT&CK, which stands for Adversarial Tactics, Techniques and Common Knowledge. It's a way for defenders to fight cyber invaders after they gain access to a network's perimeter. ATT&CK is Mitre's first detailed battle plan for understanding how cyber adversaries get into a network, and what they do after they're in — identifying and categorizing an intruder's every move inside the network. In addition, ATT&CK addresses how an organizations' technologies and information can confront the attack.

Project leaders say organizations benefit from the ATT&CK tool by having a reference point model to align with their current defenses. Organizations can use ATT&CK to create a blueprint for monitoring and assessment, to build a metrics platform, to determine cyber investments, and for continuous improvement of its cyber battle plan.

State of Missouri Office of Administration

Using Public Data to Alert Organizations of Vulnerabilities

■ Borrowing a page from a hacker who infiltrated a university's vulnerable Web-connected devices to disseminate hate speech, The Missouri Office of Cyber Security (OCS) started formulating how it could use the same technique to identify vulnerable systems on the internet for good purposes.

OCS launched a program to identify vulnerable, internet connected systems belonging not to just state and local governments, but also to businesses, utilities, and academic institutions across Missouri.

Using Censys.io, a publicly available research platform that scours the entire internet and indexes devices, open ports, and services exposed, OCS has been identifying vulnerable systems statewide.

OCS finds vulnerable systems based on banner feedback and running services. Data is reviewed and cross referenced against the American Registry for Internet Numbers (ARIN) to obtain contact information for every system identified. OCS then sends a notification to all impacted organizations. To date the program has identified thousands of software programs with expired support, and antiquated protocols that invite intruders at 161 entities and on 10,300 devices.

State of Michigan

Michigan Cyber Disruption Response Plan

■ The State of Michigan detects tens of thousands of attempts to infiltrate its government network every day. As a global hub for automotive design and manufacturing, and the home of three major research universities, it's easy to see why cybersecurity and disruption planning are top priorities. To keep pace with evolving cyber threats, Michigan developed the Cyber Disruption Response Plan (CDRP) — the first state to develop such a blueprint, which allows Michigan to establish a common framework through which all private sector and local government partners can easily and effectively protect their IT systems.

The CDRP provides Michigan's emergency management and information technology personnel, as well as stakeholders, with a plan to coordinate preparedness, response and recovery activities related to large-scale or long-duration cyber disruption. In the past, communication between the state and organizations during a cyber incident was minimal and disjointed — sometimes taking weeks for organizations to share that an incident had occurred. CDRP closes those gaps and facilitates a more open dialogue on cyber-related concerns and emerging threats.

Sallie Mae

Reducing Insider Threats with Risk Analytics

■ Some 69 percent of enterprise security executives reported experiencing an attempted theft or corruption of data by insiders during the last 12 months, according to Accenture.

At student loan company Sallie Mae, insider threats have been amplified by increasing employee turnover and more contract-based positions. To combat the problem, Sallie Mae adopted a new approach that combines machine learning, analytics and predictive anomaly detection to user behavior and access privileges that can detect and protect against insider threats, as well as external attacks that use compromised insider credentials.

Sallie Mae deployed a user behavior and entity analytics platform from Gurucul. The technology first identified outlier access, orphan and dormant accounts. Next, it was used to monitor user activity to identify anomalous behavior in both on-premises IT resources and in cloud environments. If a user downloads a confidential document under abnormal circumstances, for instance, investigators can search all other users who also accessed it to uncover events which might involve multiple actors. Excess and misaligned access to data has been reduced by up to 40 percent.

Rapid7

Access Management Automation

■ Managing employees' access to company systems gets more complicated every day as the number of user devices and entry points grows.

Data analytics solutions firm Rapid7 was struggling with two aspects of identity and access management. Both manual access reviews and manual access provisioning/deprovisioning were extremely time consuming. They didn't scale and left room for error. Rapid7's IT and IS teams developed Access Hero and ReTAP (Remote Temporal Access Protocol) — two homegrown tools that leverage automation to save the organization over 160 hours a year. Both tools were built in Ruby, back-ended by a PostgreSQL database in the cloud. The tools also reduce the company's risk exposure by ensuring access to critical business applications is limited only to users who need it.

As Rapid7 continues to add more applications and users to its organization, the number of hours saved will scale along with them.

Quest Diagnostics

Capture the Flag to Improve Secure Coding Techniques

■ Quest Diagnostics used to spend days training its developers on secure coding techniques only to reap modest improvements. Some developers didn't use what was taught to them and

others quickly slipped back into old habits. The company needed a creative approach to engage its developers and get them to retain and continually use those techniques. The solution was a Capture the Flag event that made training less tedious and more fun, while achieving optimal results.

Contestants try to break into a simulated web site, under an added Super Bowl-like atmosphere. Each day, 885 IT staff received a sports update of scores and humorous "expert" analysis cheering on the 63 developers competing. The competition has spurred contestants to push even harder for that extra edge, organizers say. Some nine out of 10 of contestants performed additional outside research to better their performance.

The event, along with monthly lunch-and-learn programs, has resulted in a 60 percent drop in new vulnerabilities reaching production applications.

ProQuest

SIFT Fraud Detection

■ ProQuest provides content, such as periodicals, newspapers and dissertations, to researchers and academics who are searching for information.

The company has seen a significant rise in fraudulent access of its content across the information industry. Libraries and other customers often rely on IP-based authentication to an entire university or public library network as the means to gate access to the content they license, but authentication was a wildcard. Most fraud engines are built to deal with financial fraud. For content search engines, a more complex set of rules, permutations and approaches was required.

ProQuest created SIFT, a fraud-detection and prevention engine focused on content-specific use cases that looks at historically "normal" usage, and learns and evolves its definition of normal usage as customers continue to use the system. It then provides a credit score-like report to subscribing applications giving them an indication of the validity of any requests for content.

After one year with SIFT, ProQuest has reduced fraudulent content loss and related security incidents.

Nexteer Automotive

NEXTINTRUST Identity Lifecycle Management

■ Like many companies, Nexteer Automotive wanted to minimize the risk of intellectual property loss and strengthen its enterprise security. A risk assessment conducted in late 2015 showed that the most critical risks involved employee onboarding and off-boarding, cloud computing governance and intellectual property protection. The company embarked on a identity lifecycle management project, called NEXTINTRUST.

Nexteer first restructured and optimized its Active Directory, and then the company acquired and deployed Okta as its identity lifecycle management tool.

Today Nexteer is working to integrate its Human Resource Information System (HRIS) and Active Directory to automatically create HRIS mastered accounts in the Active Directory and provision into Okta connected applications.

The project gives employees secure access via multi-factor authentication and increases user productivity and security. It eliminates the need to remember multiple passwords and minimizes bad practices, such as writing passwords on sticky notes. Project leaders say the company realized ROI in less than a year.

Monsanto

Creating a Cybersecurity Culture that Protects Digital Assets

■ Nearly half of all security breaches are the result of human error, according to a 2014 study. Monsanto was looking to deter those internal errors through education and awareness, so it created a "Human Sensor Network" that proactively identifies and reports potential threats.

Seven awareness campaigns were developed to address awareness gaps, and training content was translated into 18 languages to reach its global audience.

Among the program's components, Monsanto implemented a global phishing simulation campaign to provide training on how to recognize and report malicious email. It developed a new, simplified information security portal to better engage users globally. To expand the program's reach further, the company built a global network of volunteer champions to assist in delivering key awareness messages in areas language may vary. It also established a corporate ISO mailbox and an internal social media page for employees to interact directly with ISO.

Phishing simulations resulted in a 350 percent improvement in click rates and a 255 percent improvement in report rate. General reporting of suspicious email increased by 2,500 percent.

Mastercard

Mastercard Phishing Tournament

■ The Mastercard Phishing Tournament was designed to engage employees to actively look for spam and social engineering messages in their mailboxes and report them for further investigation. Each email reported is scored based on a variety of factors, and monetary awards are given each quarter to the highest-scoring participant.

Flagged messages receive special attention. Many systems merely block the sender and flag the messages to the email provider. Through the Mastercard Phishing Tournament, flagged messages are sent to Mastercard's security operations center, allowing the team to look for new versions of malware, examine senders and identify trends.

The tournament gives Mas-

tercard additional soldiers in the security fight. By using a positive approach instead of the traditional testing and re-training programs, Mastercard is turning employees into active members of the information security team.

Since the beginning of the Phishing Tournament, Mastercard has seen a 313 percent increase in the number of emails reported.

Los Angeles World Airport (LAWA)

Business Continuity Information Security

■ As one of the busiest airports in the U.S., LAX is a key part of critical infrastructure in the city of Los Angeles. To expand its protections, LAWA implemented a formal Business Continuity Process in 2013 to ensure that it could respond to emergencies and crises in a timely manner, as well as manage financial and operational risks, and avoid business and operational disruptions.

The project involved implementing and integrating LAWA's Cyber Incident Response capability and Business Continuity/Disaster Recovery capability. The RSA Archer platform was deployed to enhance collaboration between these two disparate functions. Data collected during the business-impact analysis process was used to determine critical business processes and the technology that supports them. This information was used to calculate the priority of incidents and help provide awareness of the impacted systems to include their priority and dependencies. From the incident response side, the crisis response process was activated directly from the Incident Response team allowing for faster recovery.

Kimberly-Clark Corporation

Protect K-C & Me

■ At Kimberly-Clark, information security is the responsibility of all workers. To strengthen its human firewall and increase workers' understanding of security principles, the company developed Protect K-C & Me, a global, corporate-wide information security awareness program.

In 2016, the program launched more than 30 global campaigns, including five separate Cybersecurity Awareness Month activities and events, social engineering campaigns, promotional swag distribution, training and the website launch. The program touched every employee worldwide with relevant messaging, gamification of awareness training, and a live keynote presentation by Frank Abagnale, author and subject of the movie, "Catch Me If You Can," which was viewed at regional watch parties at locations globally.

Among the results, the awareness program has distributed 320,000 phishing emails globally in 17 languages to determine the susceptibility to cybercriminals looking to infiltrate the K-C network through phishing attack. Test results showed the company has reduced risk by 12 percent.

John Muir Health

Information Security Network Visibility

■ During a risk and threat assessment of its networks in 2015, John Muir Health, a 1,000-bed health system in San Francisco, determined that it couldn't identify who was connecting to its network and whether suspicious activity was occurring on it. New CISO Tom August worked with the organization's leadership, industry peers and federal law enforcement to identify solutions that would provide visibility over the entire network.

August first had to gain a clear understanding of the enterprise's risk appetite for information security issues, which he gained through a series of discussions with board committees and executive leaders across the organization. August also created a broad platform that allows transparency into suspicious activity throughout the entire network. The health system leveraged the size and newness of each vendor to drive them to work with each other to ensure tight integration — and also integrate through the Cisco PxGrid.

Today John Muir Health is able to see across nearly all segments of their network. It's now working to establish a self-aware, self-healing network that can immediately identify, validate and react to imminent technology-based threats.

Jackson Health System

Cybersecurity via Intra-network Visibility

■ Jackson Health System declined to include a summary of their award-winning project due to privacy concerns.

Indian Health Service

Indian Health Service's Cybersecurity Program

■ Indian Health Service wanted to establish a world-class cybersecurity program in support of a vast health care network serving about 2.2 million American Indians and Alaska Natives that spans over 679 hospitals, clinics and health stations across 38 states and 567 sovereign nations.

Under a new CISO, IHS first restructured its functional capabilities and reporting structures. Next, IHS transferred the Division of Information Security employees from Albuquerque, N.M. to Rockville, Md., allowing the program to recruit cybersecurity experts from a broader talent pool. The transformation led to the creation of seven cybersecurity functional areas to address the breadth of cybersecurity needs.

As a result, the IHS has made huge strides towards innovation and substantial support for field offices and Tribal Nations by developing new and revamped functions while collaborating with health care providers. These include improved secure methods of transferring patient care data, automated logging and pharmacy dispensers, threat management, engagement and awareness training, program standardization and alignment, 24/7 incident response and vulnerability management.

INC Research

Security Training Improves Flexibility and Reduces Costs

■ In the learning-intensive and highly regulated environment of pharmaceutical clinical trials, training programs are a way of life. But at INC Research, there is great sensitivity to each additional minute of training — even for cybersecurity — that was required of its 7,000+ global employees.

Corporate executive management asked that the all-hand security training program be reduced by 50 percent from its full hour of training annually delivered in one solid block of uninterrupted time. The information security team tightened up the existing program to focus on compliance imperatives and validation of understanding and content mastery within a new delivery model of two 15-minute sessions delivered six months

apart. This model eliminated awareness topics and other helpful-but-informal guidance.

Classes now focus only on key statutory, regulatory and policy-based requirements and imperatives that must be covered annually with validity checks for all employees. It includes mastery checks for understanding, saving over 3,500 resource hours annually. The program is augmented with two-minute monthly hot-topic security awareness messages delivered via email, and continuous security messaging on the intranet home page.

Horizon Blue Cross Blue Shield of New Jersey

Domain Security Platform

■ Staying one step ahead of cyber criminals poses challenges for most health care organizations. Horizon Blue Cross Blue Shield of New Jersey (BCBSNJ) implemented the Domain Security Platform, which automatically identifies, monitors and blocks potentially malicious, newly registered external domains and websites likely to pose an elevated risk.

A homegrown solution identifies within two seconds newly registered domains being accessed from within its internal network and then monitors and blocks them as needed. All Domain Name System query information from endpoints is collected through the Horizon BCBSNJ network with the help of the ExtraHop analytics platform and Blue Coat cybersecurity and network management. Using Splunk, the organization can track via dashboard the total number of domains analyzed over time, the number of newly registered domains identified and the number blocked during a measured period.

In the first three months of operation, the platform was able to analyze 50,000+ unique domains. Of these, 412 were classified as newly created domains that warranted further investigation.

HITRUST Business Associate Council

HITRUST Business Associate Awareness Program

■ Health care organizations rely on legions of third-party vendors to handle everything from logistics to human resources, software development and financial recordkeeping. They drive efficiencies and lower costs, but they also pose potential risk to security, privacy and compliance.

The HITRUST Business Associate Council was already established to drive innovation throughout the third-party vendor supply chain while advancing practices for mitigating cybersecurity risk. So when new legislation extended the responsibilities of security and compliance to these third-party providers, the Council invited business associates to help develop an approach that would meet their needs.

Among their challenges, half of the BAs surveyed completed 100 to more than 1,000 third-party assessments annually, spending more than 10,000 hours a year. HITRUST studied the privacy and security requirements of organizations including ISO, NIST and PCI, and distilled them into a single, evolving assessment process, providing a standardized framework and tools for organizations to administer assessments. Next, the Council came up with a three-part program to overcome adoption issues and improve industry-wide understanding of the new regulations. The program is expected to not only improve cybersecurity, but also drive down costs, improve client satisfaction and inspire customer confidence.

Hershey Company

Global Identity Governance Initiative

■ As the Hershey Company expands globally, so too does its need to keep critical applications safe via a global identity governance infrastructure. Hershey recognized that a more integrated, automated and policy-driven approach to identity and access management would improve governance, eliminate unnecessary costs and give the company more agility in operations as it pursues new markets and partnerships around the world. The identity governance roll-out would need to scale and support a very diverse mix of legacy, mobile, cloud-based, IoT and other IT assets.

In just one year, Hershey completed its global identity governance project. Project leaders attribute part of the project's success to their ability to quickly gain buy-in from executives and board members by identifying how the project could alleviate constraints on Hershey's worldwide operations caused by existing, siloed ID processes.

Today Hershey can quickly on-board new employees and applications from acquired companies — a process that used to take weeks and sometimes months. SOX compliance is also easier with reporting tools that automatically generate monthly reports on who has access to what across all Hershey systems.

Health Management Systems

Asset Management on Steroids (AMOS)

■ One of the fundamentals of asset management is first knowing exactly what assets you have to secure. In 2014, members of the Health Management Systems security organization recognized an information gap between security incidences on physical assets and understanding precisely how business processes were being affected.

Disparate processes and technologies for gathering asset information resulted in confusion over where to find accurate information, uncertainty about where processes integrated, and a lack of clarity about the relationships between systems that increased downtime and the number of outages.

The Asset Management on Steroids (AMOS) project was born. AMOS ensures the consistency of information used for risk management, business operations reporting and procurement services. It requires groups to document their processes, eliminate information silos and establish standards.

Today information gaps have been closed. The operations center uses the asset information in its ServiceNow platform to facilitate monthly maintenance processes, and the security organization can accurately identify owners of assets to ensure they're quickly notified or responded to when system outages occur.

Grand Canyon University

A New Take on an Old Problem — GCU's Cybersecurity Awareness Program

■ Grand Canyon University's IT Security department has developed a cybersecurity awareness program that improved employees' ability to treat suspicious emails, phone calls and websites with an appropriate level of skepticism. Knowing that positive reinforcement is more effective than negative "gotcha" moments,

GCU employed positive steps to replace inaction with action.

In-person training has been reduced to 15 minutes in total and is augmented with brief, regular communications designed to engage and entertain while encouraging employees to take the desired action of submitting questionable items to the IT Security department. The GCU Phishing Derby caps off the awareness campaign. Timed to coincide with National Cybersecurity Awareness Month, the Derby starts with three weeks of phishing awareness tips and ends with a week-long event that offers employees a chance to win prizes for catching phishing scams.

Employee awareness has improved while decreasing instances of successful phishing and malware attacks, resulting in cost savings and increased employee productivity. What's more, employees now regularly reach out to the IT security department for guidance and clarification on all things cyber.

GoDaddy

Protect API

■ Domain name company GoDaddy has created a way to give owners of an application the control to mitigate traffic they have detected as bad, and then either drop or mitigate that traffic as needed. Protect API protects applications and services through automatic calls of an API service.

Protect API also makes it possible to automate the creation of mitigations and blackholes by exposing the mitigation appliances as a service through a REST API. This allows the owners of services, infrastructure and applications who know their traffic patterns best to identify malicious traffic and mitigate it before an outage occurs.

Protect API can also be used by other departments because it eliminates the traditional model of having to call a security operations center or CSIRT to handle an attack.

Since Protect API has been implemented, about 2,000 DDoS attacks have been automatically mitigated per month, or an average of 120-150 attacks per day. Protect API's blackhole feature has allowed internal departments to automatically mitigate brute force attacks against their applications, reducing application latency and resource usage by blocking the attack upstream automatically.

Genpact

DLP 2.0

■ Data leakage prevention (DLP) is a technology aimed at stemming the loss of sensitive information. Genpact's old DLP processes were creating a lot of false positives causing inefficiencies in the process. It also felt that reporting to senior management could be improved, so the former unit of General Electric implemented DLP 2.0

First, it leveraged its expertise in Lean Six Sigma methodologies to reduce the number of false alerts, fine-tune its detection policies and enhance the overall coverage.

Beyond DLP's technical capabilities, the company also wanted to use it to drive culture transformation and change employee behavior. Using the software's alerting feature, whenever a user tries to send confidential information on a personal account, he/ she will get a pop-up notification asking him to be sure the transmission is for business purposes.

Detailed reporting tools allow Genpact to dig deeper into each employee's online behavior, and allows IT managers to send targeted communication to high risk user groups, view metrics on response times, and improve the total time from response to resolution.

This project achieved a 63 percent reduction in the total alerts generated by the DLP system and a 25 percent reduction in the actual incidents.

Food and Drug Administration

Systems Management Center: Integrating the FDA's Cybersecurity and Network Operations Centers

■ The FDA's IT infrastructure faces persistent security threats, especially with the growth of cloud technologies and mobile devices that give new opportunities for malicious actors, trusted insiders, foreign governments and transnational criminal organizations to exploit sensitive information.

To increase its cyber defenses, the FDA Office of Information Management and Technology integrated its cybersecurity and network operations centers to form the Systems Management Center (SMC) — a non-traditional approach for the public sector.

Under the SMC construct, three teams were developed. A Tools and Alerts team handles incident management notifications and includes network, system and application monitoring tools. The Network and Infrastructure team coordinates triage and responses to incidents. The Cybersecurity Operations team monitors incident response, conducts cybersecurity analysis and proactively addresses imminent threats to prevent risk exposure and disruption.

Today the SMC provides near real-time cybersecurity capabilities and risk management methodologies to protect sensitive data and information systems. Project leaders say it has also become a model for collaboration and transparency across the entire FDA enterprise.

Flowserve Corp.

Modernizing Infrastructure Security Through Micro-Segmentation

■ Flowserve, producer of engineered seals, pumps and valves, provides services to some of the most essential organizations in the nation, including nuclear and military facilities. As threats to critical infrastructure increased, Flowserve decided to take a different approach to modernizing its security posture to protect heavily regulated production facilities that provide services to nuclear and military facilities, as well as services to other mission-critical commercial environments such as oil and gas production.

Flowserve leveraged micro-segmentation software to isolate its most important and regulated environments. Micro-segmentation works across a heterogeneous environment, rather than using traditional physical segmentation which relies on firewalls, VLANs and physical infrastructure. The approach allowed the security team to load software onto network devices, with a single management console coupled with bits of code that run on IP devices. This allowed system managers to layer on controls that decide who gets to do what, and easily enforce those rules at the network packet level.

Workers now have access to data on a need-to-know basis, and endpoints are protected from unauthorized users.

FICO

Build Security In and Measure Success

■ Credit score company FICO has come to know that getting security right requires more than just the technical pieces of reporting issues that are found and fixing them. It believes security also encompasses business, social and organizational aspects.

To fully embrace these synergies, FICO implemented the Build Security in Maturity Model (BSIMM) framework that allows the company to measure its program against peers, make improvements across the software lifecycle and monitor its risk posture.

The BSIMM framework captures and makes available an overall understanding of the diverse software initiatives and methodologies in the organization. It provides a yardstick for describing the most important elements of a software security initiative and allows FICO to measure different methodologies or those that operate at different scales.

Project leaders say the framework has created a common vocabulary that allows all development teams to reach across silos and disrupt the reliance on "tribal knowledge." What's more, the average time to correct critical and high-priority issues has been reduced from 32 days to five days.

Esri

SOC Reinvigoration — Increase Efficiency of SOC Operations

■ Esri, the geospatial technology organization, has implemented a portfolio of security products to protect the many diverse digital assets of both the company and its customers. The portfolio identifies more than 10,000 incidents/alerts per week. This presents the company with significant challenges when trying to analyze and respond to these alerts with limited resources and time.

Esri set out to increase its efficiency in responding to alerts and to reduce costs in its security operations center. The organization acomplished its goal by harmonizing multiple automation capabilities. For instance, the automation added with the Demisto platform, which automates security operations and incident management processes, complements Esri's existing SIEM and network monitoring solutions, improving efficiency for the SOC team.

Project leaders say that automating the mundane tasks allows human analysts to focus on decision-making vs. collecting evidence. This reduces a major portion of the time that Esri teams would spend running separate tools and performing repetitive tasks.

With automation and collaboration, the volume of alerts that require active human review has been reduced from 10,000 per week to about 500.

Educational Testing Service

Securing the Software Development Lifecycle

■ Educational Testing Service (ETS) develops, administers and scores more than 50 million tests annually in over 180 countries across 9,000 locations worldwide.

Results of ETS educational tests affect eligibility for scholarships and acceptance to universities. For professionals, obtaining critical professional certifications hinges on test results. To keep systems safe, ETS set out to identify and eliminate security flaws. This critical step was the start of new approach to a comprehensive enterprise security program.

ETS developed a systematic and repeatable process that helps the company detect and correct vulnerabilities and security flaws in the software it develops. The process was created with the input of many software developers, and it treats security vulnerabilities the same way that developers routinely treat software defects. Rather than leading developers to consider security as something separate from software development, this approach integrated security into the standard, daily tasks of developers — finding and fixing bugs. This made removing security vulnerabilities seem less foreign to them.

The project significantly reduced ETS' security risks by integrating new services and tools into the ETS software development process.

Department of Homeland Security

Automated Indicator Sharing

■ In January 2015, the White House directed the Department of Homeland Security to develop automated indicator sharing as a way for private sector entities and government departments and agencies to share cyber threat indicators, such as malicious IP addresses or the sender address of a phishing email.

DHS moved quickly to develop Automated Indicator Sharing (AIS) and rolled out its initial offering in November 2015. AIS receives, sanitizes and redistributes indicators and defensive measures, allowing participants to identify and mitigate cyber threats in real-time.

DHS leaders say the project's goal is to commoditize cyber threat indicators and enable everyone to be better protected against cyber attacks. That would mean adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber attacks.

When Congress passed the Cybersecurity Act of 2015 in December 2015 with some new and more specific requirements, the system was modified again. While AIS won't eliminate sophisticated cyber threats, leaders say, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

Creative Artists Agency

■ Leveraging Operational Intelligence and User Behavior Analytics to Migrate to the Cloud

Creative Artists Agency declined to include a summary of their award-winning project due to privacy concerns.

Celgene Corp.

Data Loss Prevention

■ Global biopharmaceutical company Celgene was looking to reduce its cybersecurity risk, protect sensitive information, classify vast amounts of data and determine who has access to it.

Project leader Michael Stanley and his team launched the data loss prevention project, which included a governance model, a new strategy and new technology to address defined requirements for identifying sensitive data at rest, data in use and data in motion.

The project required an unprecedented amount of collaboration among core business groups in identifying their data and defining its appropriate use — a difficult task considering the biopharmaceutical environment is highly collaborative and is constantly sharing new data. The team leveraged technology to help identify

and track the movement of sensitive information, and distinguish who has access to the information to ensure its security.

So far, DLP has been embraced by business units. As the number of identified sensitive documents has increased, the incidence of inappropriate use, such as confidential information sent to a personal email account, has decreased.

Cancer Treatment Centers of America

We ARE Safe — Information Security Awareness and Training

■ The leaders at Cancer Treatment Centers of America (CTCA) believe that information security is an extension of patient safety. Security technologies protect its assets, but the key defense is educating employees about cyber attacks and creating a culture of safety. CTCA's enterprise-wide initiative, "We ARE Safe — Accountable, Reliable, Empowered," is the framework for addressing incident response through security awareness training. The program develops essential competencies and establishes a process to stay ahead of potential breaches.

It also fosters an employee culture that's "highly reliable" for safety — meaning achieving and sustaining a high performing organization with an internally driven safety focus — paying more attention, communicating more clearly and thinking more cautiously.

Project leaders say the program has enabled CTCA to treat information security with the same degree of seriousness as preventing infection. Over a ten-month period, the number of messages flagged by users, and added to anti-SPAM tools increased from one or two per month, to five to ten per week.

BNY Mellon

Smart Docs Cyber Custodian

■ The U.S. home loan system is underpinned by hundred of millions of collateral documents. BNY Mellon is required to control and manage these documents throughout the term of a loan. The previous process for managing documents had weak tracking capabilities and a manual audit procedure.

Smart Docs Cyber Custodian automates the identification and management of collateralized loan documents — combining the internet of things technology with digitization for compliance and risk management. The adoption of Smart Docs ensures that collateral files are transferred in a timely manner and all impacted parties are able to quickly obtain the documents when needed.

The new approach involves scanning the documents into a designated electronic cabinet location. The physical document is afixed with an RIFD tag so it can be tracked as it moves throughout BNY Mellon. The project reduces the manual handling of documents for verification and certification by 70 percent, reducing labor expense and preventing document loss.

Blue Cross and Blue Shield of North Carolina

Managed File Transfer Realignment

■ Blue Cross and Blue Shield of North Carolina (BCBSNC) is part of a highly regulated industry with many business and trading partners with whom it shares data. Like most companies, BCBSNC developed governance processes on the intake side of new file transfers, but lacked the same level of controls to ensure the transfers were decommissioned when no longer needed.

Its Managed File Transfers Recertification project was initiated to recertify all existing transfers and develop a sustainable, automated model for the future that leverages existing processes and technology used for certifying user access.

The challenge was to automate a tedious and ineffective process and align it with existing effective business processes. By improving how the file transfer information was cataloged, BCBSNC developed a master file capable of integrating with its existing IAM tool.

Once the master file repository was complete, a feed was established between the repository and its IAM tool. This provided business owners a simpler means of attesting to their file transfers. The result is a sustainable workflow to prevent manual recertification that provides increased visibility into BCBSNC's file transfers.

The Blackstone Group

Automating Malware Investigations

■ As a global investment firm with more than 21 offices around the world, Blackstone and its security team see 30 to 40 malware alerts in a single day. Blackstone's incident response team investigates each malware alert as if a compromise has already occurred, a process that requires 30 to 45 minutes to fully address each alert if done manually. Automation was the answer, but despite Blackstone's own expertise in scripting and automation, developing this capability across a large set of security vendors became difficult to maintain. As each vendor changed the API for their product, the automation scripts also had to change.

Blackstone selected Phantom as its security automation and orchestration platform. The platform integrates existing security technologies and provides a layer of connective tissue between otherwise disparate systems. The project has reduced the time required for Blackstone's response team to investigate malware alerts. The automated malware investigations now take about 45 seconds, freeing the team to focus on analysis and resolution.

Beebe Healthcare

Organizational Security Management

■ Beebe Healthcare, a nonprofit healthcare system in Lewes, Del., established a dedicated security team in March 2015 to focus on all areas of cybersecurity threats, compliance, risk assessment and mitigation, effectively going from 0-100 mph in a very short time. The team has improved security awareness, threat reduction, and proactive incident response efforts for the health care system.

Among its successes, the team established a security awareness and training program that included a phishing assessment in addition to personal, departmental and community outreach. The goal was to identify employees' risk profile for phishing susceptibility. The initial assessment showed that more than 29 percent of the employees would fall for a well-crafted phishing email and were unaware of reporting or handling procedures. In one year, with the IT security department's active training, new employee orientation and continued resilience testing, employees' "phish risk" percentage dropped to 8 percent.

Banesco Banco Universal, Venezuela

Securing Internet Banking Transactions

■ Banesco Banco Universal, Venezuela's largest bank, needed a centralized system to prevent, monitor and ensure the security of its online banking service in real time.

The security team at Banesco Banco designed, developed and implemented an application, called the Predictive Console, that integrates the online banking system with databases, legacy systems and other monitoring systems. Team leaders say the project was based on the concept of a security model applied in layers, allowing a simple solution to integrate and improve coverage in the prevention and control of fraud events. This tool does not require modifications to the business logic, and it reuses existing security mechanisms to strengthen the effectiveness and functionality of the solution. It uses a risk engine based on the behavior of customers, using connections and financial profiles.

With the solution in place, Banesco Banco saw fraud reduced by 75 percent from 2015 to 2016, and the number of fraud events decreased by 84 percent.

AT&T

Storm 2.0 Threat Analytics Platform

■ Telecom giant AT&T has come up with a next-generation threat analytics platform that transitions to big data technology, collects a broader dataset, increases performance and adds analytical capabilities. The platform's mission is to utilize this data to collect events, detect security threats, initiate remediation and, ultimately, protect AT&T and its network from compromise and malicious activity.

The Storm 2.0 Threat Analytics Platform project involved a custom big data implementation. The project team designed a Hadoop-based cluster, creating a unique big data stack. The team then implemented this stack in a 110 data-node cluster and successfully migrated more than five billion records per day to the new platform.

The team integrated existing threat management tools, including HP's ArcSight SIEM, the proprietary AT&T Malicious Entity Database, Anomali's ThreatStream and the internal AT&T RCloud analytical library. This created a platform that acts as an ecosystem of security threat analytics.

AstraZeneca

Cloud Control Point

■ AstraZeneca, a global pharmaceutical company operating in over 100 countries, put collaboration at the center of its IT security strategy with a secure, global cloud collaboration platform. The challenge then became how to keep track of what data is in the cloud, where it is going, and who can access it.

The security team enlisted Skyhigh Networks' cloud access security broker as a central control point for all cloud traffic, sanctioned and unsanctioned. AstraZeneca uses Zscaler as their inline proxy to monitor web traffic across users, devices and locations and to protect employees from malicious or compromised sites. Skyhigh integrates with Zscaler to process proxy logs and provide visibility into AstraZeneca's cloud usage, as well as the individual risk ratings of each service.

Today the IT department has granular visibility into every kilobyte of data sent to the cloud and control with data loss and collaboration policies. At the same time, they removed the need for VPN access. Employees, patients and medical professionals worldwide can securely share data in the cloud.

Amkor Technology

Ransomware Inoculation

■ Amkor Technology, a semiconductor services provider, needed a way to prevent ransomware from becoming a weekly fire-fighting event.

Amkor InfoSec group embarked on a project to mitigate damage from future ransomware campaigns and allow for quicker recovery. Amkor first analyzed the way ransomware, a highly scripted attack virus, performed after detonation, then it tailored a solution that both retarded the effects of ransomware and allowed for easier and

faster recovery. Similar to an inoculation, the solution doesn't prevent the infection, but rather blunts the virus's capabilities and allows for faster recovery.

Among the project's features, the group created a GPO that will block common ransomware command execution after detonation within Windows OS. It also created a new policy on the centralized storage device blocking encryption commands utilizing the most common encryption extensions used by ransomware. On the recovery side, Amkor ensured that all critical data is on shared directories, which are snapshotted every four hours to allow for a worst-case, four-hour data loss.

Project leaders say this is a program most companies can implement with little money and one that makes them immune from 99 percent of the known ransomware.

Aflac

Ducking Threats — Aflac's Automated Threat Intelligence Control System

■ Aflac witnessed a significant increase in the volume and velocity of new security threats. So the insurance provider embarked on a mission to create a custom-built threat intelligence system capable of consuming large amounts of threat data and, in turn, use that data to protect the environment and inform security decisions.

Part of the solution involved maximizing the use of API integration. The threat intelligence platform uses APIs to communicate and share information between platforms. Numerous APIs push data between systems that otherwise would have had to be manually loaded in batch. With this approach, the system has been able to automatically consume threat data, assign confidence ratings and deploy it to security infrastructure block lists.

Partnering closely with Splunk, Aflac was also able to integrate its threat intelligence data with its user behavioral analytics solution to enrich its advanced analytics.

Within a six-month period in 2016, the threat intelligence system has blocked more than two million connections, with fewer than one dozen false positives.

AECOM

Improving Employees' Ability to Spot Phishing Emails by 300 percent in 18 Months

■ When engineering firm AECOM first measured the phishing awareness aptitude of its 100,000 employees, almost 30 percent of them failed to identify the scams. In response, the firm designed a phishing awareness program that focused on raising awareness, reducing the fail rate, helping employees understand how to get help and to feel no shame about coming clean when inadvertently clicking on phishing emails.

For the next 18 months, its education and awareness campaigns would focus wholeheartedly on phishing, with a few other topics sprinkled in to help keep content fresh. Project leaders say the entire campaign came at very little cost but required a huge amount of dedication, creativity and influence across the company. All channels were coordinated by leveraging the influence of the CISO, executive support in business lines and regions, collaboration with internal communications and marketing, befriending the graphics team and soliciting help from every corner of the organization.

As a result, AECOM reduced its phishing fail rate from 29.9 percent to 6.7%. ■