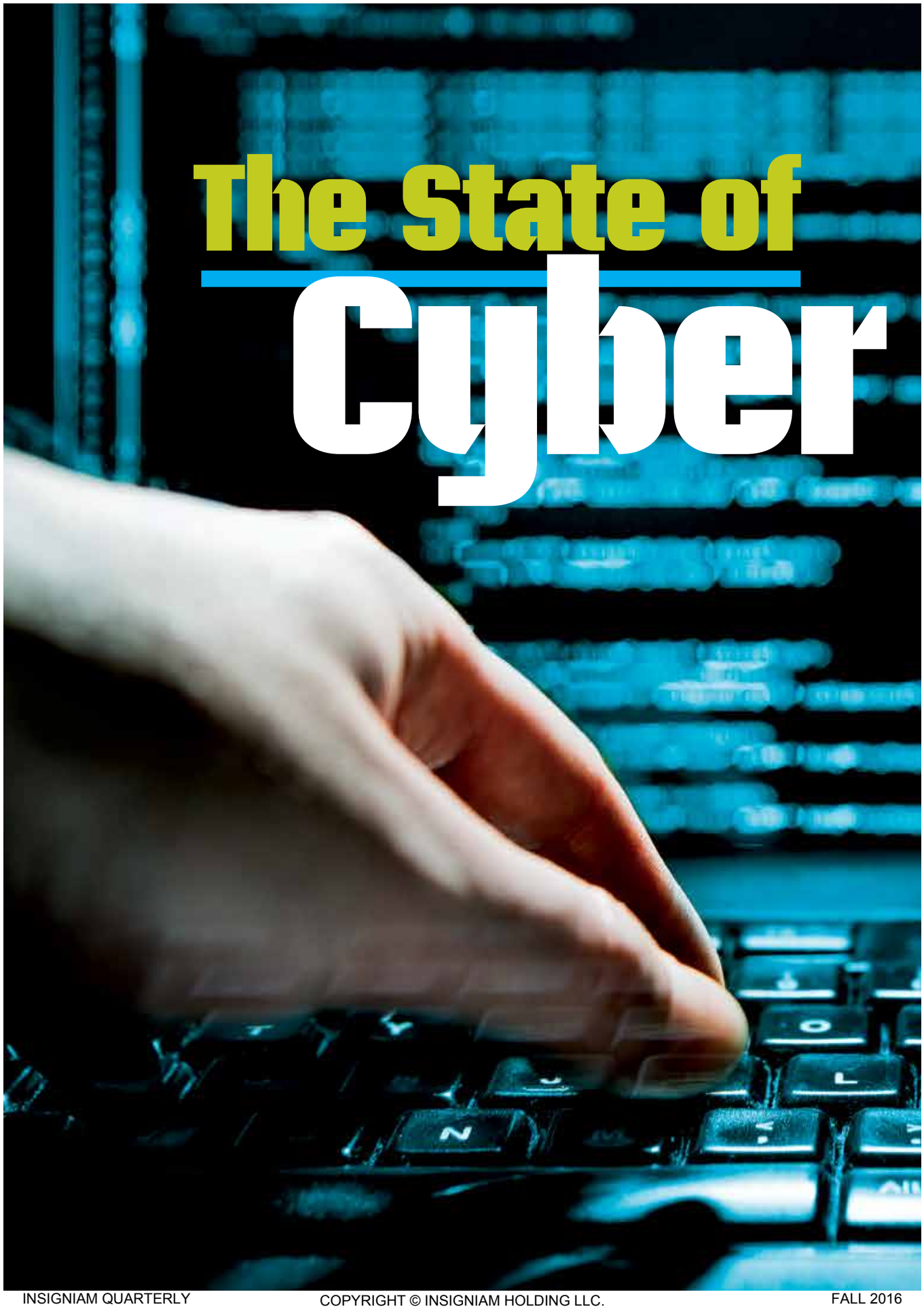
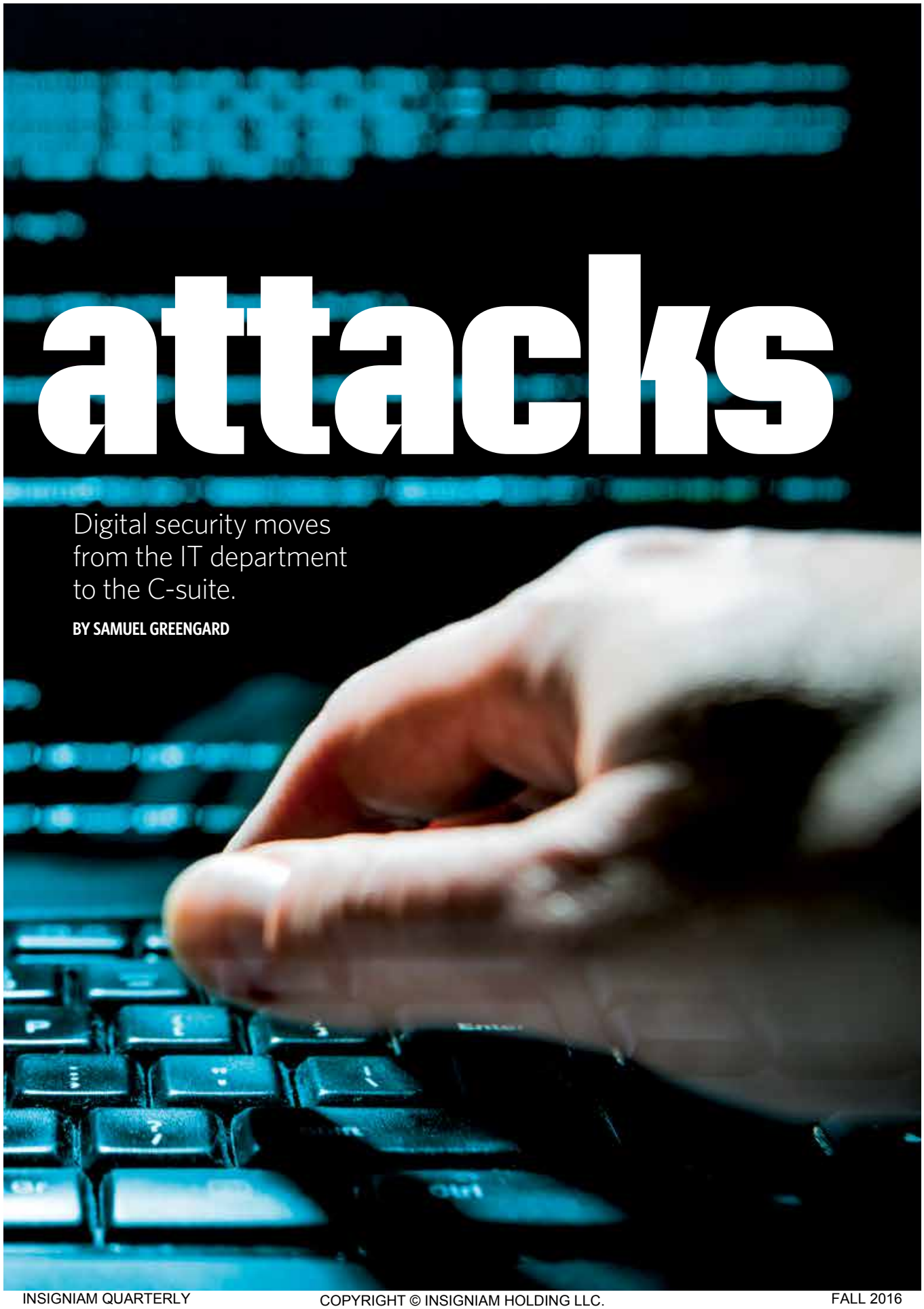
The State of Cyber





attacks

Digital security moves from the IT department to the C-suite.

BY SAMUEL GREENGARD

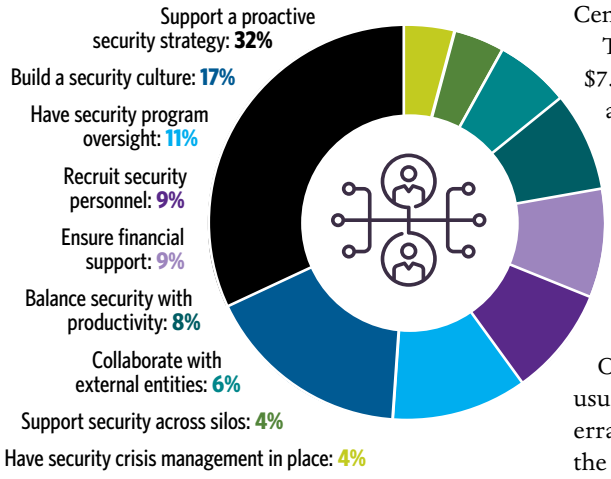
More than 200,000 homes in the Ukraine were left without power for hours last December when a group of hackers took 30 regional substations offline. It was the first major power network to be taken down by a cyberattack—and is an unsettling example of the escalating impact of cyberattacks in recent years.

The list of targets breached in the past two years alone reads like a veritable "who's who" of business and government: MySpace, eBay, Bangladesh Bank, British Airways, Facebook, Japan Airlines, the Korea Credit Bureau and the Australian Immigration Department, just to name a few. The message seems clear: No organization is safe. Including yours.

According to the World Economic Forum's *Global Risks Report 2016*, business leaders in eight countries, including Japan, Germany and the United States, view cyberattacks as the top operational risk. "While traditional industries are using digital systems to introduce greater automation and efficiencies, hackers and attackers are using the same technology to completely revolutionize the way crime takes place," says Raj Samani, CTO for EMEA at Intel Security and a member of Europol's Cybercrime Centre advisory group. "Malware and USB sticks have replaced guns."

The average annualized cost of cybercrime for an organization is $7.7 million globally, according to a report from the Ponemon Institute and Hewlett-Packard. But cyberattacks trigger indirect costs as well. According to cybersecurity leader FireEye, 76 percent of U.S. consumers are likely to stop purchasing from a company if a data breach is found to be linked to a failure to prioritize cybersecurity. More than half have a negative perception of companies that suffer a breach.

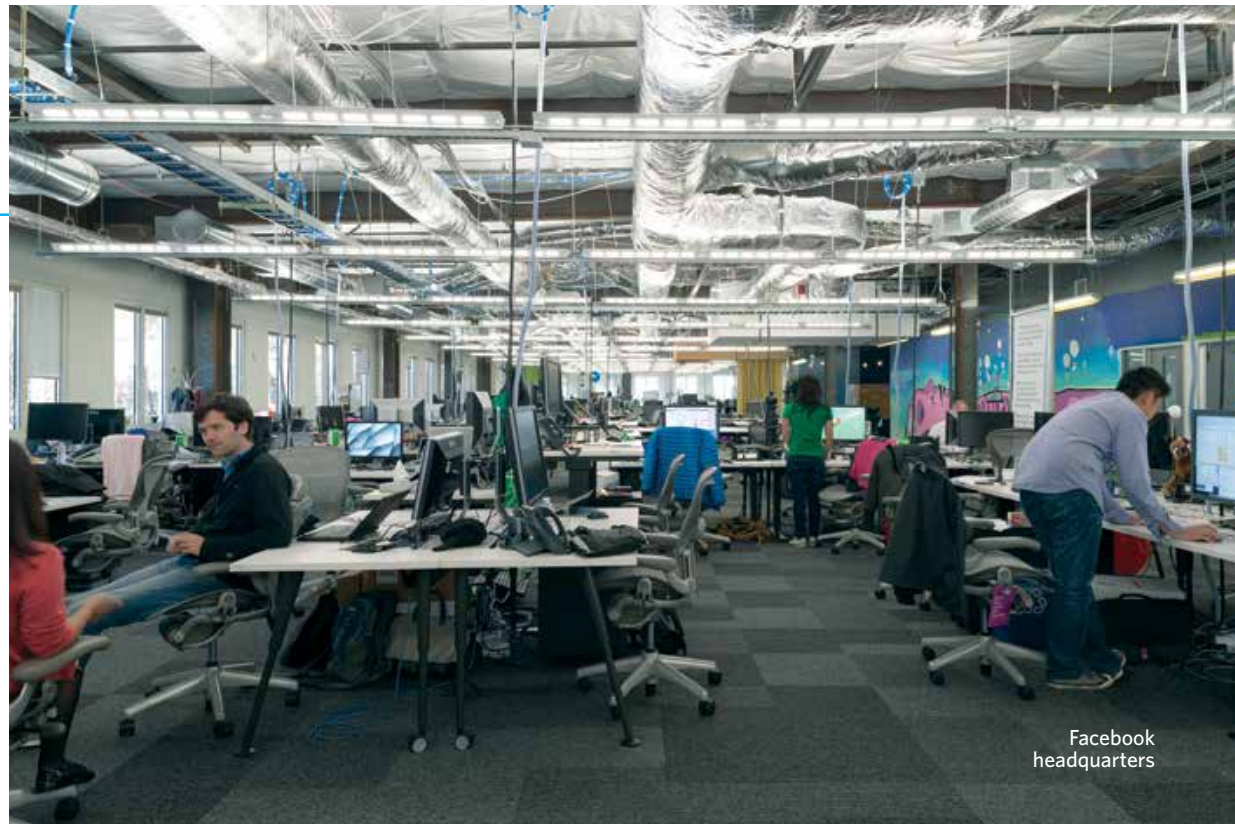
What is the most important thing the C-suite/ board can do to support data security?



Source: Economist Intelligence Unit, *Data security: How a proactive C-suite can reduce cyber-risk for the enterprise*, 2016

The New Threat Landscape

Only a decade ago, computer viruses and other malware were usually little more than a nuisance. An infected system might display erratic behavior or lock up. In most cases, antivirus software could fix the problem and restore operations to normal. However, over the last few years, the nature and danger of threats has changed dramatically. "Attackers and threats are much stealthier," says Troels Oerting, group



Facebook headquarters

PHOTO COURTESY OF FACEBOOK

chief information security officer (CISO) at U.K.-based Barclays. "They are focusing higher up the food chain and looking to inflict major damage."

So-called "low" and "slow" attacks—which may involve cybergangs lurking in systems for weeks, months or even years—are designed to collect data and information drip by drip until the perpetrators have what they need to carry out a theft or attack. "We have moved from noisy and easy-to-detect attacks with a large and obvious footprint to methods that are more difficult to detect," says Joshua Goldfarb, vice president and CTO at FireEye.

No less disconcerting is the fact that some of today's critical infrastructure relies on old and often obsolete systems and software. This makes modern protections, such as data encryption, malware detection and security patches and upgrades, difficult to implement. Until IT system upgrades are made, attackers see easy targets.

Even HVAC systems in modern buildings might pose a threat for intrusion. In some cases, criminals may enter these systems and, if they are tied into a primary computer network, break into data stores and files.

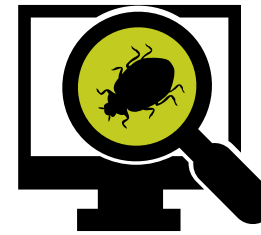
It is a simple yet profound concept. "Basically, any time you put anything on the network, you are giving people access to that device or that object," Mr. Goldfarb says. And the risks increasingly extend beyond mobile phones and direct network connections. "Connected Internet of Things devices can now serve as the launch point for attacks."

"While traditional industries are using digital systems to introduce greater automation and efficiencies, hackers and attackers are using the same technology to completely revolutionize the way crime takes place. Malware and USB sticks have replaced guns."

—Raj Samani, CTO for EMEA at Intel Security and member of Europol's Cybercrime Centre advisory group

Start With Security in the C-Suite

Clearly, the external threat facing companies is real and growing. But there is an internal threat as well: complacency. Despite a plethora of cautionary tales, many organizations still fail to



Cyber Pest Control

There is no panacea for all cybersecurity threats—and that means companies must be willing to try innovative approaches to battle unseen digital foes. One such approach on the rise is bug bounty programs, in which organizations pay white-hat hackers to identify weaknesses in their cybersecurity systems.

Standard-fare tech companies such as Yahoo, Google, Facebook, Mozilla/Firefox and Microsoft have well-established bug bounty programs. Collectively they have paid out more than $13 million in fees to hackers for finding vulnerabilities.

Over the past couple of years, however, new players and non-tech giants—including Deutsche Telekom, Samsung, Tesla, Starbucks, General Motors, the U.S. Department of Defense and Spotify—have been getting into the game. According to crowdsource cybersecurity agency Bugcrowd's *State of Bug Bounty 2016* report, "Overall, organizations from more 'traditional' industries have seen year-over-year growth [in bounty programs] of over 217 percent on average, including financial services and banking, automotive, health care, education, telecommunications, hospitality, real estate, utilities and consumer goods."

In August, Apple said it would pay rewards of up to $200,000 to researchers who find critical security bugs in its products.

And earlier this year, Uber announced it was launching a bounty program, offering fees of as much as $10,000 for critical issues. The ride-sharing company also provides the hackers with a "treasure map" that clues them in to some of the more vulnerable components of the system.

"Uber's in 70 countries around the world now, so a one-size-fits-all model is definitely never going to work for us," Samantha Davison, manager of security awareness at the company, said at this year's Infosecurity Europe conference.

Yet despite the apparent surge in bug bounty interest, Bugworld's report found that 94 percent of companies on the Forbes 2000 have yet to launch a vulnerability disclosure or bug bounty program.

proactively respond to the looming threat of cyberattacks. According to a 2016 report by Barclays and the United Kingdom's Institute of Directors, 91 percent of business leaders believe cybersecurity is crucial, but only 57 percent say they have a formal strategic framework in place to protect their organization.

"Our report shows that cyber must stop being treated as the domain of the IT department and should be a boardroom priority," Richard Benham, author of the report and CEO of the United Kingdom's National Cyber Management Centre, said in a statement.

In fact, support and awareness from both the C-suite and the boardroom are crucial factors when it comes to successfully impeding security breaches. Growth of cyberattacks and breaches was reduced by more than 50 percent in companies that had a security strategy backed by a fully engaged C-suite and board of directors, according to a 2016 report by The Economist Intelligence Unit.

"It's difficult to obtain funding for essential systems and training if you don't have the support and buy-in of the C-suite and the board of directors," Mr. Goldfarb says. Adds Mr. Samani: "It's impossible to

eliminate all risk. But the ability of all business leaders to understand risk in real-world ways typically translates into a better security framework."

Waqas Akkawi, CISO at global relocation and moving services provider SIRVA, agrees. "The common approach is to view security technology as discrete tools and systems," he says, adding that organizations must instead adopt a more integrated approach. "They must be smarter about understanding threats and building out a risk-based cybersecurity framework. It must be built into every business venture, project and process, and involve business and supply chain partners."

For a growing number of organizations, bridging the gap between top leaders and the tech and IT teams has led to the creation of chief security officer or CISO roles in the C-suite. The U.S. government is following suit: President Barack Obama announced in February his intention to hire the country's first CISO.

These top IT executives do more than just assess risk and design risk-based frameworks. They also provide regular briefings to the C-suite and the board, interface with business leaders across the enterprise and serve as the champion for security in everything they do. And, importantly, they understand the need to balance cybersecurity bells and whistles with what is most critical for a particular organization.

"There is no way any organization can build out a cybersecurity framework that will deliver 100 percent protection," Mr. Goldfarb says. "No enterprise has unlimited resources. So it's important to prioritize dangers, systems and alerts by understanding the top risks for an industry and a specific business."

Know Thy Enemies

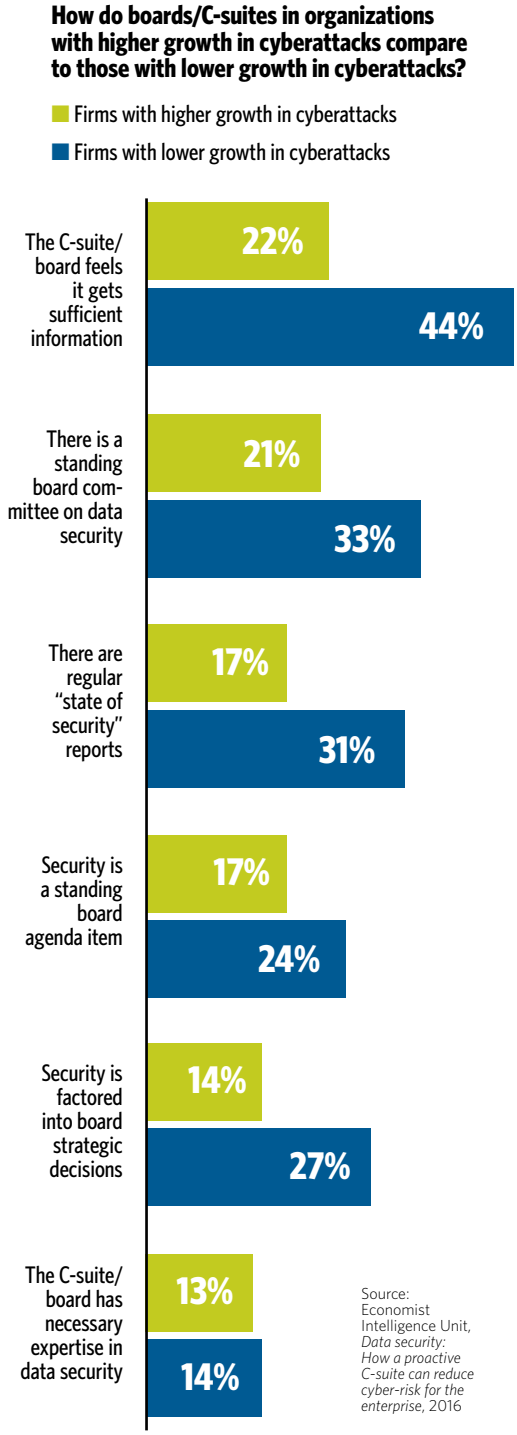
Before organizations can decide how to best battle cyberattacks, they must first identify the enemy. At Barclays, combating cyberattacks starts with an assessment of the organization's adversaries and their potential intent and motivations. "We use this analysis to estimate probabilities and impact of attacks," says Mr. Oerting, who is also a member of Interpol's Global Cybercrime Expert Group, where he advises the general secretariat on cybersecurity programs and operations.

Once that assessment is complete, Mr. Oerting and his team look at their defense, assessing vulnerabilities and controls. "In our response, we run 24/7 security and attack monitoring including incident response, coordination and defense," he says. "We focus on securing our 'crown jewels' and controlling those with privileged access to our most valuable assets."

For most organizations, a strong defense means implementing a multilayered approach using a group of technologies combined with

"It's difficult to obtain funding for essential systems and training if you don't have the support and buy-in of the C-suite and the board of directors."

—Joshua Goldfarb, vice president and CTO, FireEye



Source: Economist Intelligence Unit, *Data security: How a proactive C-suite can reduce cyber-risk for the enterprise*, 2016

the right controls and processes. This includes traditional tools such as firewalls, antivirus systems, endpoint security, data loss prevention and desktop virtualization.

At a most basic level, Mr. Goldfarb says it is crucial to reduce the number of privileged accounts and establish strong authentication, including the use of two-factor authentication, to reduce the odds of a breach. "It is one of the most effective protections possible, and it's a highly effective tool when cyberthieves have obtained a password through social engineering or other methods," he explains. "If they are unable to provide the rolling code or other token through another device, they cannot get into the network."

Companies should also use end-to-end encryption whenever possible, while data is both at rest and in transit. However, if an attacker steals an employee's credentials and uses them to log in, it will be possible for him or her to gain access to the system and view decrypted data. That is why, as basic as it sounds, organizations need to institute a policy to de-provision old accounts promptly to prevent former employees from retaining access to files and data.

"Former employees and disgruntled employees are a serious, often-underestimated threat," Mr. Oerting explains. One global cybersecurity firm, Stroz Friedberg, has made headlines with its new software SCOUT, which aims to detect insider threats *before* they happen. At the behest of executives, SCOUT will comb through a company's emails using an algorithm based on linguistic tells and flag employee emails containing indicators of serious security threats. Although Stroz declines to identify most clients, it has reported working with companies such as Target, Neiman Marcus, Facebook and Google, according to *Fortune*.

Yet perhaps the most crucial piece of the cybersecurity defense puzzle is simply making sure employees and others using systems have adequate training on security best practices. That includes how to spot phishing emails, manage authentication and passwords, and protect laptops and mobile devices that can easily be stolen or compromised.

"It's important to have critical controls in place so that people can't download and install toolbars and apps that represent a real risk," Mr. Akkawi says. "But it's also important for employees and contractors to understand how and when they are engaging in dangerous behavior."

Next-Gen Protection

Beyond using currently available cybersecurity tools, organizations are now sizing up the defensive powers of an emerging slate of new technologies.

One promising area is analytics and behavioral analysis,

"It's impossible to eliminate all risk. But the ability of all business leaders to understand risk in real-world ways typically translates into a better security framework."

—Raj Samani

including advanced persistent threat analytics. Banks and credit card companies have used predictive analytics to detect unusual behavior and fraud for the last decade, and the technology is steadily expanding into cybersecurity as many traditional network-monitoring security tools gain more advanced analytics capabilities. The technology is also starting to utilize machine learning and artificial intelligence. Predictive analytics "can view patterns that are otherwise imperceptible to humans," Mr. Goldfarb says. "It's an area of great promise."

Earlier this year, MIT and machine-learning startup PatternEx created a platform called AI^2 that can predict 85 percent of cyberattacks. The system scours data for suspicious activity by grouping it into meaningful patterns. Those patterns are then presented to human analysts who confirm the accuracy of the identified cyberattacks, and the machine uses the feedback to improve its analysis.

IBM is similarly taking on cybersecurity with the help of AI—specifically its Watson supercomputer. The company plans to partner with eight universities that have advanced cybersecurity programs, including the University of Ottawa and the University of Waterloo, to train Watson in the language of cybersecurity before the cognitive cloud-based service is launched in beta form later this year.

Perhaps the most anticipated new tool, however, is blockchain—a data structure that uses cryptography to create a digital ledger of transactions and share it in a secure way among a distributed network of computers. Originally created to support the virtual currency bitcoin, the technology is now being adopted and tested by a growing number of companies, including 40 of the world's top financial institutions, according to *The Wall Street Journal*. But banks are not the only ones expressing interest. In May, a U.S. panel on cybersecurity and cyberspace appointed by President Obama heard testimony on the technology from experts at IBM, and the United Kingdom recently inked a deal with cybersecurity firm Guardtime to develop blockchain solutions for critical infrastructure systems in the country.

Despite these promising solutions, there is no quick fix for cybersecurity threats on the horizon. Every company needs to approach the challenge with a unique tool set. A combination of end-user security awareness, simulations, ongoing testing and more advanced and integrated solutions spanning everything from mobile devices to applications is the best recipe for strengthened security. As Mr. Samani says: "It's all about developing a framework and the right tools and technologies for minimizing risk." **IQ**

IBM's Watson supercomputer


Predictive analytics are increasingly being used to combat cybersecurity threats.