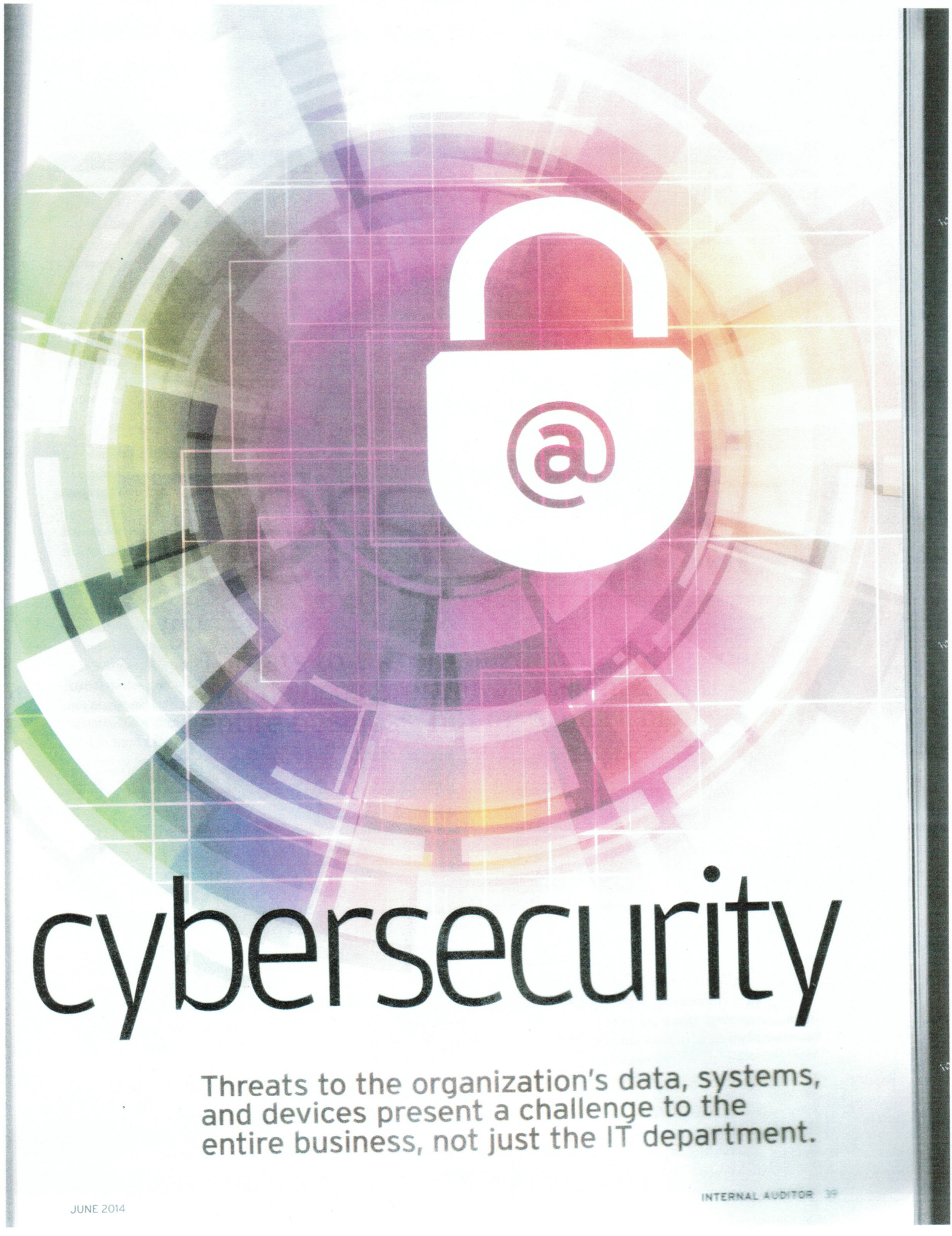
Businesswide

Arthur Piper

Cyberrisk and cybersecurity have come of age. From the board and management, to the chief information officer and the chief audit executive, organizational leaders typically now discuss cyberthreats not solely as an IT problem, but as a fully fledged business risk. And this elevation of concern and attention is introducing not just new ways of understanding the persistent threat of cyberattack, but different, more dynamic ways of addressing the exposures it creates.

Survey after survey ranks cyberthreat among the top 10 risks that keep business executives awake at night. But bracketing off the risk in this way is no longer relevant. Take the Allianz Risk Barometer on Business Risks 2014, for example. It lists cyberthreat separately from business interruption and supply chain risk; loss of reputation and brand value (from social media and elsewhere); and theft, fraud, and corruption. But risk from cyberattack arises in these areas too, meaning that the problem cuts across almost 80 percent of all business activities the survey identified.

That is one reason why the scale of the threat is hard to quantify. Cyberattacks cost the world economy between US $300 billion and $1 trillion in 2013, compared to US $600 billion from drug trafficking, according to software



cybersecurity

Threats to the organization's data, systems, and devices present a challenge to the entire business, not just the IT department.

company McAfee. Jeffrey Kosc, partner at business law firm Benesch, Friedlander, Coplan & Aronoff, says the cost of a single data breach can include anything from the expense of fixing the problem that caused the loss and dealing with business interruption, to the legal costs of handling any investigations launched by state and federal regulators, the fines they may impose, and the class action lawsuits filed by people whose data may have been compromised.

"People forget that compliance with security procedures does not always mean you are secure," Kosc says. In particular, throwing money at large security systems is likely to be just the beginning of the costs businesses face if they are not also being proactive and continually improving their security approach.

What businesses need to focus on are the specific types of attack they face today and the weaknesses inherent in their business practices, culture, and IT systems. Internal auditors armed with such knowledge can help management develop better controls and assess their effectiveness. But internal auditors also need to be engaged at a more strategic level, knowing what the board's approach to security is, working proactively with systems administrators, and getting involved with new IT implementations at an early stage. Because internal auditors work across all areas, they are ideally placed to understand cyberthreat as a business risk and help the organization tackle it effectively.

> Internal audit needs to understand the organization's security posture and determine where the organization is going with security."
>
> James Reinhard

SEE "The Threat of Attack" on page 78 for more on cybersecurity

PRIMARY THREATS

The main threat most businesses face comes from two umbrella risks: denial of service attacks (DoS) and data security breaches. The first of these is probably the hardest to predict and protect against. That is because the people who IT security specialists call "threat actors" can be individuals, hacker groups—such as Anonymous, the high-profile cyber-activists—criminal gangs, or even state actors who have a grudge against the business or organization they target.

"It's like the 1970s sit-in protests," says E.J. Hilbert, managing director for Kroll Cyber in the U.K. "They're saying, 'I'm making my personal belief known in a world where I want instant gratification. If you don't fix the problem right now, I'm going to attack you.'"

In a typical DoS attack, a website, email, or network will be flooded with so many requests, or so much data, that it will cease to function. In a distributed DoS attack, an organization's computers may be taken over and used to attack a different target. That could mean hundreds or thousands of compromised computer networks are joined together to immobilize a single business.

Organizations are not defenseless. The U.S. Computer Emergency Readiness Team (US-CERT) advises businesses to implement secure firewalls and up-to-date antivirus software. They should keep open communication channels to Internet service providers too so that they can work together if an attack is in process. Organizations need to have effective network monitoring to detect unexpected spikes in activity and rapid response plans to take action against any attacks, US-CERT says.

Data security breaches often are much easier to prevent. Companies can be compromised because staff members fail to follow basic procedures, such as not clicking on the Web links contained in spam emails that could admit a virus. Several studies have claimed that between 80 and 90 percent of all such breaches are avoidable by taking simple steps, including using effective passwords to access sensitive parts of the network. Although this has been standard advice for more than a decade, password management company SplashData says the most common security passwords in 2013 were "123456," "password," and "12345678"—combinations that any cybercriminal's algorithm could crack

The average business faces more than 100 attacks each year, costing US $11.6 million annually, according to security research firm Ponemon Institute's 2013 Cost of Cyber Crime Study.

within minutes. Given that people also use the same password for many devices and applications, a single breach can have wide-ranging effects.

FRESH THINKING

Defending against these sophisticated attacks requires a different way of thinking about cyberrisk, says Rob Sloan, head of response at Context Information Security. "If you want to get the company working under the same security strategies, you have to start thinking about educating the board," he says. "The board needs to accept this isn't simply an IT problem, this is now a business risk and the business areas must accept that they need to work together."

The first step, he says, is to decide on the level of risk the organization is prepared to accept around its data so that everyone in the business understands the risk appetite in relation to information. Second, he says, the board should understand precisely what the organization's critical assets are. In other words, what information is vital for its long-term financial health and what would the impact be if these assets were stolen or compromised? Finally, the business should build its approach to security accordingly, including understanding the nature of the traffic passing through the network so that it can detect and act on anomalies.

This strategy could help businesses categorize and segregate data more clearly, so that sensitive information is accessible by fewer people and is stored more securely for the relevant time period. Even if the organization's security systems are breached, it makes it less likely for the perpetrators to roam freely around the network taking the data they want before they are discovered.

Having this focus on the organization's overall risk appetite and understanding what data is crucial to the business' success is also essential if internal audit is to be effective. "Internal audit needs to understand the organization's security posture and determine where the organization is going with security," James Reinhard, audit director at Simon Property Group in Indianapolis says. "If we know those things, we can put our resources where the highest cyberrisks are in the corporation."

He says internal audit should work with the security administrator every time new security procedures are put in place, or each time the business implements new software, at least at the steering committee and project meeting levels. It should be involved in the reviewing of design specifications and functionality and testing, he says.

Reinhard admits that internal audit resources and the number of specialist IT auditors is often limited, but he sees most value added where the function takes a business risk approach to cybersecurity. "You really need to take a practical standpoint and do a business and IT impact analysis, and do risk assessment on both of those aspects together," he says. "What are the business risks? What are you trying to resolve? And are you covering those business objectives?" He says simple 10- to 15-hour audits on password security to check how people are managing them, devising control self-assessments, and sending out reminders can all make a big difference in the way people behave.

In a world where business supply chains are intimately connected, internal audit plays a critical role in making sure cybersecurity standards are upheld throughout the entire business infrastructure, says Dave Roath, PricewaterhouseCoopers partner and head of the firm's IT Risk and Security Assurance Practice. That can include making sure that due diligence is performed around suppliers' cybersecurity practices and developing service agreements that allow internal audit to audit those vendors' arrangements. Similar issues can arise through the use of cloud services, where it may be difficult for the business to know who has access to company data and where geographically it is held. That knowledge can help determine which

SOCIAL ENGINEERING

More sophisticated data security breaches contain elements of social engineering, and threat actors have recently been targeting individuals within organizations whom they believe might have access to particular types of data. Law firms, for example, often advertise the partners working on specific projects, such as competitive mergers and acquisitions, or stock market offerings, inadvertently sending out a clear message as to who might have valuable data. Although these individualized attacks are very formulaic, they are difficult to detect because each is unique and so has no "signature" that can be picked up by antivirus software.

Typically, the target receives an email from someone he or she knows, such as the CEO, either from a general email address (e.g., Yahoo or Gmail) that carries that person's name, or a corporate address that has already been compromised. That message contains either a link to a site that the recipient is encouraged to click, or an attachment that he or she is asked to open. If the recipient carries out the request, malicious software could give the attacker a back door to that computer – or if the attacker is particularly sophisticated, the whole corporate network could be made accessible.

data is best held on the cloud and which should be stored securely on the organization's own network.

Nancy Haig, director of internal audit and compliance for a global consulting firm, suggests that, in addition to reviewing data security controls, auditors confirm that corporate insurance coverage has been recently reviewed by experts, and that a policy has been added to specifically include cybersecurity events. "Traditional corporate liability policies do not cover these events because data is not tangible property," Haig says, "and even standalone cyber policies should be carefully reviewed to determine that all associated costs of a breach would be covered." She adds that auditors should ensure coverage limitations—such as unencrypted laptops or mobile devices—have been avoided, so that there are no surprises.

The changing nature of cyberattacks requires a better understanding of the worth of business-critical data.

SECURITY FRAMEWORK

To date, there has been a fragmentation of approaches to cybersecurity in different business sectors, and organizations have set their systems according to the demands of their industry and its regulators. In February 2014, that began to change when the U.S. National Institute of Standards and Technology (NIST) published its Framework for Improving Critical Infrastructure Cybersecurity. The document is the result of a yearlong consultation between business and government to devise a common language for dealing with cyberrisk.

"Cybersecurity is becoming more of a business issue, and the framework reflects that," says Adam Sedgewick, senior IT policy adviser at NIST. In that light, the framework aims to promote a culture of continuous improvement, rather than seeing the solution to cyberthreat as static—something that can be handled simply by buying new equipment. In addition, the document is aimed at business leaders so that they can understand what a good security system looks like and be able to communicate that throughout the organization.

Sedgewick says internal audit has a central role to play in helping the business align the attributes of good cybersecurity programs with the business' own goals. "The internal audit community should understand the decisions an organization is making on cybersecurity and help tie that to an organization's larger risk profile," he says. Because internal audit already deals with the business' financial and reputational risks, for example, they are in an ideal position to help coordinate those different perspectives.

This approach will be crucial if the board and executive management are to understand cyberrisk as a business issue. Dealing with the changing nature of cyberattacks also requires a better understanding of the worth of business-critical data and the way that people use that information across the organization to create value. Internal audit can join those dots and help everyone see the bigger picture.

Arthur Piper is a writer who specializes in corporate governance, internal audit, risk management, and technology.

Traditional corporate liability policies do not cover [cybersecurity] because data is not tangible property."

Nancy Haig

Cybersecurity is becoming more of a business issue, and the [NIST] framework reflects that."

Adam Sedgewick