The chief risk officer, Nathan, put it plainly to CEO Tom: “To say that cybersecurity presents complex challenges is an understatement. The scope of risk to sensitive information has grown exponentially during the twenty-first century. Those risks not only involve technical factors, but human, cultural, and legal factors, as well as economics. Of course, the profession of cybersecurity has struggled to grow in tandem with these challenges. But nobody has the resources to ensure complete data security. Figuring out where security investments are justified requires a sophisticated understanding of the risk landscape.”

THE LANDSCAPE OF RISK

Hardly a day goes by when the evening news does not include a report about a major institution reluctantly announcing that its files have been hacked. The stories tend to follow a familiar pattern: expressions of official regret, attempts at reassurance, and pledges to do whatever is required to prevent its future recurrence.

Attacks on institutional and corporate databases have become the new normal. A generation of workers comfortable with information sharing has also grown accustomed to its negative consequences. The capabilities of cybercriminals continue advancing at an alarming pace. And the losses associated with major data attacks, which run into the millions, are increasingly seen as just another cost of doing business.
At the same time, however, there is a growing understanding of those consequences. A movement in the leadership ranks of both business and government agencies to manage cyber risks more effectively and to improve the resilience of security tools already in place, has followed. This is a welcome development because, until fairly recently, most senior managers and board members regarded cybersecurity as essentially a technical problem for their IT departments—not as an existential issue requiring greater investment as well as the engagement of personnel throughout the organization. That said, however, some of the issues really do involve the organization’s network technology.

Technology flaws—whether in design, encryption, event logging or software malfunction—create opportunities for attackers to infiltrate an organization’s technical infrastructure. Understanding and realistically assessing the vulnerabilities of an organization’s system components is essential. But it is people, far more than technology, that present the greatest risks.

**THE PEOPLE FACTOR**

Most high-profile attacks on corporate servers and institutional networks originate outside of the victimized organizations—in many cases from halfway around the world. But the network openings that allow cyber attackers to burrow in, infect databases, and potentially take down an organization’s file servers, overwhelmingly originate with trusted insiders. There are three categories of insider threats, as illustrated in Figure 7.1.

![Three types of insider threat](image)

**FIGURE 7.1** Three types of insider threat identified by the Information Security Forum (ISF)

*Source*: Copyright ISF. Used with permission.
In some cases, those insiders are driven by malicious intent—the desire to enrich themselves through the sale of sensitive data or to retaliate for perceived slights or mistreatment in other instances. Deceptive behavior—sometimes referred to as social engineering—is used to trick employees into divulging proprietary codes, passwords, or other private company information. There are also cases where an organization’s third-party contractors, vendors, or temporary workers, essentially privileged users, have been responsible for their client’s network breaches, either through malice or by accident.

However, according to a survey of Information Security Forum (ISF)\(^1\) members, the vast majority of those network openings were created innocently through accidental or inadvertent behavior by insiders without any intention of harming their employer. In a number of cases, that vulnerability was the ironic result of a trusted employee doing something seemingly ordinary like taking files home to work on in their spare time.

That risk is exacerbated by personal mobile devices. Welcome or not, they have become inexorably tied into corporate information systems. And their use frequently reflects their owners’ relaxed consumer habits.

Therein lies the rub: the cost associated with data leaked, hacked, stolen, or compromised for most private individuals is comparatively low—perhaps limited to personal embarrassment. But for a multinational corporation, it can be huge. Marketing plans, product road maps, pricing strategies, personnel records, customer account data, confidential correspondence, and other types of sensitive information, if stolen, corrupted, or held hostage for ransom can have a disastrous impact on an organization’s operations and its reputation. It can also enrage loyal customers who expect—and the courts require—that their private information remains private.

Indeed, for anyone, irrespective of where they may be located, if they operate using personal information relating to European citizens, the stakes have just been significantly raised. The EU’s General Data Protection Regulation (GDPR)\(^2\) has penalties of up to 4 percent of global turnover just waiting to be applied to organizations unfortunate enough to be hacked and suffer the loss of EU citizen personal information. The EU GDPR comes into force in 2018 and adds another layer of complexity, not to mention potential cost and associated resources, to the issue of critical information asset management that so many organizations are struggling to come to terms with.

As a result, there is now a much clearer recognition of both the immediate and longer-term costs associated with cyber attacks. Identifying an organization’s vulnerabilities is key to developing effective responses. Organizations must deploy a multiphase process, to assess cyber threats—whether these threats are deliberate, unintentional, or the results of environmental incidents such as floods or power failures. Here is how it works.
A STRUCTURED APPROACH TO ASSESSING AND MANAGING RISK

There are different tools and software available in the market to help risk managers assess their information vulnerabilities. Symantec, Trend Micro, NetIQ, ISF, and others are reputable firms with applications and techniques focused on different aspects of risk management. They all have satisfied users. A robust information risk assessment methodology should not simply be a piece of software but a comprehensive procedure to identify, analyze, evaluate, and manage a variety of information risks throughout their organizations in a structured manner, and then to generate risk profiles in terms that are meaningful to the organization’s business. See Figure 7.2, which illustrates the six phases of the ISF IRAM2, which identifies the distinct stages of risk management.

In fact, the need for a structured approach to the identification and management of risk has never been greater than in today’s always-on, constantly communicating, cyber-enabled business environment. A realistic and disciplined assessment of the worst-case scenarios for business in advance of this need, is to prioritize the organization’s investments in defending against cyber attacks.

Such an approach typically involves six phases:

- The first provides guidance for generating an integrated view of information risk, ranging from an organization’s business processes through to its technology.
- The second offers guidance for realistically assessing worst-case scenarios—the potential business impact if information assets become compromised.
- The third involves mapping different types of threats, both malicious and accidental, that could potentially affect the business.
- The fourth involves assessing your vulnerabilities to different threat events and the strength of any controls already in place.

The six phases of IRAM:

A. Scoping → B. Business Impact Assessment → C. Threat Profiling → D. Vulnerability Assessment → E. Risk Evaluation → F. Risk Treatment

FIGURE 7.2 The six phases of the ISF IRAM2

Source: Copyright ISF. Used with permission.
The fifth stage evaluates the organization’s risk appetite and likelihood of a successful threat in light of the previous findings.

The sixth and final phase involves developing practical approaches to addressing the information risks which have been identified.

In essence, it provides companies with a highly structured and practical method for assessing risks to guide critical business decisions. By taking a comprehensive view of risk exposure and focusing attention on the most significant ones, organizations may predict and prevent attacks instead of simply reacting to them after they occur.

**SECURITY CULTURE**

Accurately assessing the attributes of cyber threat and an organization’s resilience to them involves examining factors including organization capability, commitment, people competence, and user privilege patterns. Common threat attributes could include simple deception used in phishing attacks, stealthy taps into unsecured wireless networks, or using “accidentally misplaced” removable media to inject malware into the targets network.

But one of the most significant factors is the organization’s culture, which often mirrors the society where it is located. For the multinational organization, that means taking into account the ways in which different cultures view protecting data and the way in which those cultures respond to directives about safeguarding digital devices and commingling corporate and personal business on those same devices.

A study commissioned by Cisco almost a decade ago found that risky behavior and rampant disregard for their organization’s security policies occurred at alarming rates among employees in all parts of the world, although some were worse than others. Those personal patterns do not appear to have changed that much. But a 2016 international survey by PricewaterhouseCooper offered some encouraging news about an important turnaround at the institutional level. It found that 65 percent of those organizations surveyed now collaborate to improve their cybersecurity, 69 percent use cloud-based cybersecurity services, and many more follow a risk-based cybersecurity framework, most frequently ISO 27001 guidelines.

There is also a generational difference. Generation Y employees, as a whole, do not feel as though requirements for securing sensitive information apply to them as much as they do to their more senior colleagues. Instead, among recent entrants into the job market, the prevailing view is that it is the organization’s job to make sure information is secure—not the individual’s.
But while there has been a welcome growth in security awareness among senior management, the view that security is the responsibility of higher-level employees is frequently misplaced. A recent Nasdaq survey highlights alarming gaps between awareness and accountability at the highest levels of global enterprises: too many board members and executives are unable to understand security briefings and unwilling to accept responsibility for data breaches. Indeed, for many organizations, the more senior someone is, the less aware they tend to be of the way data needs to be secured. Some senior executives seem to think they’re immune from security threats altogether.

Another reason that deferring to senior colleagues on security matters may be misguided is that those senior colleagues are of the same generation that formerly nourished their newer employees’ relaxed attitudes. Most of today’s employees have gone through educational institutions where they are encouraged by their mentors to share information. Go to any university in the United States, and you will be given ready access to a host of information sources all across the country.

But while we encourage people to share information, we do not teach that there are also security considerations around the ways they use that information. So when those students eventually become employees, they are thrust into a completely different, and far less forgiving, information security environment.

**REGULATORY COMPLIANCE**

In highly regulated environments, like financial services, there are a number of statutory requirements an organization needs to comply with. And that has tended to drive institutional behavior; they’re compliant because they have to be. But if you are going to avoid innovative attacks, compliance will not necessarily help. A compliance-driven strategy might satisfy the authorities, but it will do little to discourage a creative hacker.

At the same time, there are banks and other organizations that see compliance only as a starting point. That is because by the time a regulation goes into effect, it is usually out of date. Compliance regulations come about because of something that happened in the past. They have been put in place to prevent a past act from repeating itself. It is like preparing today to win a previous war.

However, cyber is different than other types of risk. Cyber is exceptionally fast moving. It is not like slip-and-fall injuries or vandalism, embezzlement, or any of the other conventional risks an organization faces. A lot of the cyber attacks that take place are unprecedented. They have never been seen before. As a result, if you follow only a compliance approach, you are
looking backwards and leaving yourself open to attacks that seem to come out of nowhere.

It is a balancing act. First, you really do have to be compliant. And second, you have to do everything reasonable to protect your organization’s mission-critical information. That realization has prompted some leading organizations to take a slightly different approach. In the past, they have tried to protect things like devices; they have tried to protect networks; they have tried to protect the perimeter on the assumption that if you can stop somebody from coming in, you can be secure.

Unfortunately, there are plenty of holes in those perimeters. There are lots of ways a hacker or attacker can come in. Maybe it is through a third party; perhaps through a faulty device, possibly through human error, maybe through an outside contractor, or even through an insider who either willfully hands over information or innocently makes a mistake that allows a hacker to gain access. A number of intrusion-penetration test methodologies are commercially available to help identify holes at different points in the network.

**MATURING SECURITY**

As recently as 10 years ago, cybersecurity was primarily a function of IT departments. Organizations tended to treat their data protection as a technology matter—one best left to its techies. The organization’s established risk managers tended to focus instead on the organization’s traditional insurance coverages. And its product line managers rarely felt any connection to the cybersecurity function. That is all starting to change.

There are different levels of maturity in cybersecurity across enterprises. The most mature ones have moved into a broader risk function. Those coming up the maturity curve still tend to view their work as part of IT, where security concerns were initially focused. But as the economy assumes a more resilience-oriented approach to preventing and recovering from attacks, we need to view security as a holistic business issue—not just an IT issue.

In an ideal world, there should not be any barriers separating data security from the organization’s core business functions. In reality, however, most security departments are still not consulted—nor are they viewed as business enabling. Instead, they are viewed as being the “No” guys—the ones who prevent things from happening and keep employees from downloading their favorite software, logging onto sports and entertainment websites, going onto social media, or checking their Gmail.

However, once an organization has been attacked, it is likely to get the religion of security rather quickly because a hack is typically more than a
transient business disruption—it impacts your brand, your reputation, your operations, and creates costs for cleanup, forensics, investigations, and so on. In organizations that have been attacked, as well as their competitors, there typically follows a sharp uptick in their focus on data security.

PRIORITIZING PROTECTION

Years ago, securing an organization’s information was synonymous with safeguarding its computers. But the recent explosion of devices and users and interconnection channels has made it essential to shift from a focus on devices—which actually form the perimeter of a network—to their core: the information it contains.

Today, with so many devices and so many users touching the data, protecting them all is impossible. Instead, organizations need to focus on what is important from a business standpoint: protecting mission-critical information, regardless of who might want to access it, irrespective of the devices they might be using, and no matter where they might be coming from.

That represents a sea change from the earlier device-centric safeguards. Today, the approach to security begins and ends with the organization’s data. How do I protect my data? Which data is truly mission critical? And who really needs to access it?

Going through that exercise leads you to think about data in a somewhat different way: What are my organization’s crown jewels? How do I need to protect them? What behaviors am I trying to protect against? Who actually needs to access this information, and when?

Safeguarding an organization’s mission-critical information is a process involving a number of moving parts—technology, leadership, culture, policy, environment, and more. They are all subject to change over time, and adversaries who want to attack those assets are constantly on the lookout for any opportunities those changes create. Regularly and systematically assessing your organization’s technological defenses, its potential business impact scenarios, its matrix of threats, and the resilience of its current configuration to potential attacks are all essential to developing a pragmatic plan to resist and, if worse comes to worst, to recover from an assault on your most critical data.

CONCLUSION

The following cyber risk management statement represents those organization capabilities CEO and board expect to be demonstrated in terms of identifying, analyzing, and evaluating (i.e., assessing) cyber risks.
IDENTIFYING, ANALYZING, AND EVALUATING CYBER RISKS

The organization realistically assesses the vulnerabilities of its digital system components not just for technology flaws (such as in design, encryption, event logging or software malfunction) but for human factors. Trusted insiders present the highest risk (motivated either by malice or more commonly by accident) as well as third-party contractors, vendors, or temporary workers (essentially privileged users). The organization commits to a robust and structured approach to assessing and managing risk and an information risk assessment methodology. This involves a six-part approach to (1) generating an integrated view of information risk; (2) realistically assessing worst case; (3) mapping different types of threats, both malicious and accidental; (4) assessing vulnerabilities to different threat events and the strength of any controls already in place; (5) evaluating risk appetite and likelihood of a successful threat; and (6) developing practical approaches to addressing the information risks that have been identified. Other factors examined include organization capability, security culture, commitment, people competence, user privilege patterns, technology, leadership, policy, and environment. There is a balance between regulatory compliance and doing everything reasonable to protect mission-critical information. Cybersecurity maturity avoids barriers separating data security from the organization’s core business functions and does not rely on device-centric safeguards. The focus begins and ends with the organization’s data: how it is protected, which data is truly mission critical, what behaviors need to be protected against, and who really needs to access it and when.

NOTES


ABOUT THE INFORMATION SECURITY FORUM (ISF)

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit organization whose members include many of the world’s Fortune 500 and Forbes 2000 organizations. It is dedicated to investigating, clarifying and resolving key issues in information security and risk management by developing best-practice methodologies, processes, and solutions to meet the business needs of its members.

The ISF offers a trusted and confidential environment in which members’ in-depth knowledge and practical experience can be shared. This collaborative approach enables the ISF to harness the collective insights and knowledge of its members to deliver comprehensive leading-edge solutions that are both pragmatic and effective.

The ISF has developed a proprietary, second-generation Information Risk Assessment Methodology known as IRAM2. It is not simply a piece of software. Rather, it is a comprehensive procedure—largely the product of members’ input—that helps companies identify, analyze, evaluate and manage a variety of information risks throughout their organizations in a structured manner, and then to generate risk profiles in terms that are meaningful to the organization’s business.

ABOUT STEVE DURBIN

Steve Durbin is managing director of the Information Security Forum. His main areas of focus include strategy, information technology, cybersecurity and the emerging security threat landscape across both the corporate and personal environments. He is a frequent speaker and commentator on technology and security issues including cloud, Big Data, the Internet of Things and the impact of cybersecurity on business growth and profitability.
Formerly at Ernst & Young, Steve was responsible for the entrepreneurial markets business in Europe, Middle East, India, and Africa. He has been involved with initial public offerings and mergers and acquisitions of fast-growth companies across Europe and the United States, and has also advised a number of Nasdaq and New York Stock Exchange–listed global technology companies.

Previously, as global head of Gartner’s consultancy business, Steve developed a range of strategic marketing, business, and IT solutions for international investment and entrepreneurial markets. He also served as a Digital 50 advisory committee member in the United States, a body established to improve the talent pool for Fortune 500 boards around cybersecurity and information governance. In 2014, he was ranked as one of the top 10 individuals shaping the way that organizations and leaders approach information security careers.