Pixsooz/Getty Images

A framework for improving cybersecurity discussions within organizations

Jason Choi, James Kaplan, and Harrison Lung

Clear and frequent communication is essential but often lacking in companies' cybersecurity programs. Here's how security professionals can create tighter bonds with some critical stakeholders.

The entire world is going digital; virtually every type of cross-border business transaction now has a digital component.[1] Companies' use of digital technologies is opening them up to new relationships with customers and business partners, and new business opportunities. But, as recent headlines have made clear, the very act of connecting to the outside world increases organizations' risks exponentially—of project failure, of data breach, or worse.

In this era of global digital flows, companies must take all possible steps to build robust cybersecurity capabilities. Protection strategies cannot be focused solely on

[1] For more, see *Digital globalization: The new era of global flows*, McKinsey Global Institute, February 2016.

technological controls and remediation plans. Companies must invoke the human element as well. They must seek to build digitally resilient cultures in which cybersecurity is not an occasional concern but an everyday task for core business stakeholders at all levels, inside and outside the organization (Exhibit 1). In such cultures, discussions about asset protection are proactive rather than reactive, and communications among critical decision makers are open and frequent.

Trust among business stakeholders is a necessary component of digitally resilient cultures; without it, organizations will have a difficult time successfully shielding the customer data that nowadays is so critical for achieving business goals. The board needs to trust that senior management has a long-term view of cybersecurity, with a strategic road map and plans in place to adequately protect information assets and IT systems, regardless of where and how new threats emerge. The business units, the IT organization, and the cybersecurity team need to trust one another enough to get to a mutual agreement about how security protocols can be integrated into daily business processes without creating operational challenges and frustrations. Companies need to have faith that external partners—for instance, cloud vendors—are willing and able to protect shared data and infrastructure. And finally, government agencies need to trust that companies are proactively reporting breaches and sharing information that could help them spot and thwart major cyberincidents, particularly those spanning multiple industries and countries or involving state-sponsored attacks.

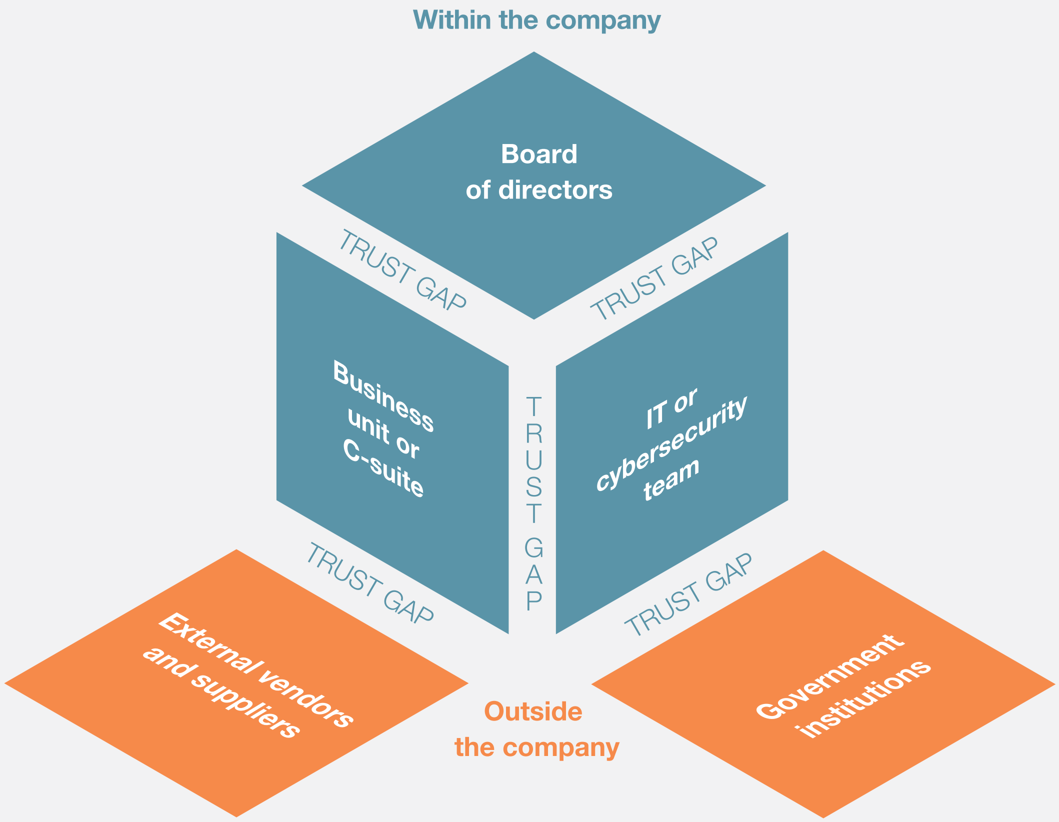
Trust among these stakeholders is often missing for a number of reasons, including conflicts of interest and lack of insight into the complicated technologies and concepts associated with cybersecurity. If business and technology professionals don’t have a common understanding of cybersecurity issues, for instance, they may never properly execute security protocols, and their adoption of even the latest and greatest technologies may never yield the desired results.

In this article, we explore the communication gaps that exist among these stakeholders, and we suggest ways to bridge these divides. We share our insights on the dysfunctional relationships that can develop within the corporate ecosystem, while acknowledging that the most complicated trust gap still exists between companies and customers. Clearly, no cybersecurity program can ever be 100 percent foolproof; the threat landscape is changing too quickly. But we believe the companies that can facilitate trusting relationships and productive discussions about how they secure critical business assets will be better prepared to respond to ever-advancing cyberthreats.

Trust gap 1: The board and the C-suite

The dynamic between board directors and the senior management team can be fraught for any number of reasons, but first on the list is that cybersecurity is usually not a top item on many board-meeting agendas; often it is presented as part of a larger discussion of IT issues, if it is mentioned at all. Many board directors therefore tend to be less informed about cybersecurity technologies and issues than they may be about standard financial and operational issues—apart from what they read in newspapers about the latest corporate or government security breach. They come to the table with questions about the company’s cybersecurity programs. For instance, are the company’s most critical assets being adequately protected, and is there a robust response-and-recovery plan in place if a breach does happen? Who actually owns the

EXHIBIT 1 **Cybersecurity trust gaps can exist on many levels across the corporate ecosystem.**



cybersecurity agenda, and does that individual or team have the appropriate level of power and influence to mobilize the required resources?

A trust gap develops when senior management falls short in answering these questions. In some cases, the senior-management team may not be able to properly opine on governance issues because it has not clearly defined owners for particular cybersecurity issues and activities—for instance, who should manage safety training modules: the leaders in the business units, or in IT? The senior-management team may not have the right data in hand to properly quantify the current levels of risk the company faces and present a comprehensive mitigation plan to the board. Or the members of the C-suite simply may not communicate with the board often enough when it comes to cybersecurity issues: despite the fact that transparency is a new norm in most companies, our research suggests that only 25 percent of companies present IT security updates to the board more than once a year, and up to 35 percent of companies report this information only on demand.

Finding common ground

Members of the C-suite need to create more transparency and forge stronger communication with board directors. Senior leaders should formally assess the maturity of their cybersecurity programs regularly and present their findings to the board at least annually but preferably even more frequently. This exercise should involve a structured consideration, by members of the senior-leadership team and others in IT and the business units, of the severity and likelihood of attacks on major corporate assets. For instance, which internal and external threats are the biggest, and what is the business value at stake (Exhibit 2)?

Through this process, the C-suite can develop a dashboard or regular reporting mechanism to inform the board about past and present levels of risk and the potential effects of risk on the company. Such dashboards and reports should use clear, simple language rather than the acronyms often favored in technology discussions. And they should always include impact statements: What are the financial, operational, and technological implications of emerging threats to the business? By establishing regular reports about cybersecurity, the C-suite can signal the importance of the topic to the board—and the need to set cybersecurity apart from the board's review of general IT initiatives.

Trust gap 2: The business units and the IT organization

Trust-based relationships among individuals in the business units, the IT organization, and the cybersecurity function can be difficult to maintain—in part because these groups sometimes work at cross purposes. The cybersecurity team may impose certain safety protocols that are inconvenient for employees in the business units, or otherwise impede their daily operations. Consider your own reactions to IT requests to change passwords—coming up with yet another password that has the required length and complexity and that you can still remember. Such exasperation can escalate from the individual level to the business-unit level. (See sidebar, "How agile development can help close the trust gap between the business and IT.")

For their part, cybersecurity teams may get frustrated with business colleagues who complain about these perceived inconveniences and don't recognize the important role they play in defending digital business assets. When cybersecurity teams grant data- and system-access rights to employees, they must trust that individuals will act appropriately. The IT group expects employees to be generally aware of how corporate systems work, how their actions online are traceable, and how to safeguard their credentials and information. But, in fact, company insiders can pose significant cybersecurity risks. One cybersecurity study noted that 60 percent of all cyberattacks in 2015 involved insiders, an increase of 5 percentage points from the previous year.[2]

Bulking up training efforts

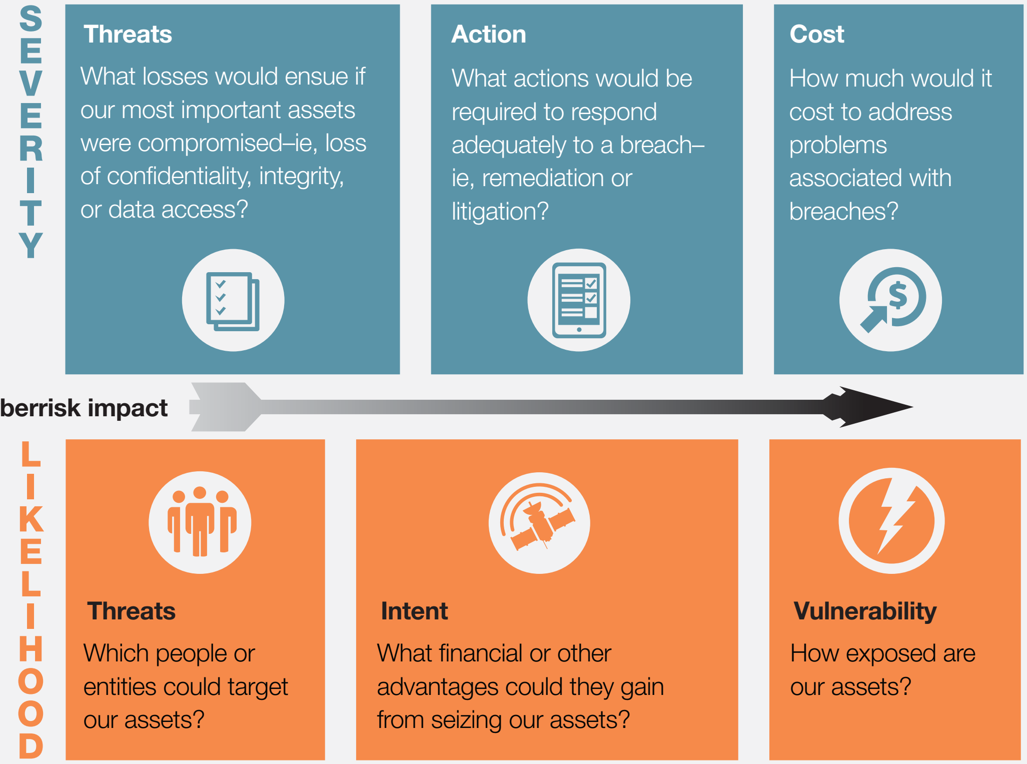
To help close the trust gap between the IT and cybersecurity function and the business, the organization can provide comprehensive cybersecurity training to staffers at all levels. This might include dedicated town-hall meetings, workshops, and training modules focused on identifying varying types of cyberthreats and outlining appropriate responses when employees witness suspicious activity.

Such training can help business-unit employees understand the rationale for cybersecurity protocols and raise their awareness. Even more important, it can signal to the business units

[2] 2016 *Cyber Security Intelligence Index*, IBM X-Force Research Index, IBM, 2016, ibm.com.

EXHIBIT 2

Companies should continually monitor assets for the likelihood and potential severity of cyberattacks.



SEVERITY

Threats
What losses would ensue if our most important assets were compromised–ie, loss of confidentiality, integrity, or data access?

Action
What actions would be required to respond adequately to a breach–ie, remediation or litigation?

Cost
How much would it cost to address problems associated with breaches?

Cyberrisk impact

LIKELIHOOD

Threats
Which people or entities could target our assets?

Intent
What financial or other advantages could they gain from seizing our assets?

Vulnerability
How exposed are our assets?

that cybersecurity is a shared responsibility. Anyone who has access to confidential data and systems, at whatever level, must play an active role in ensuring their safety.

Companies may also want to develop mechanisms by which IT and cybersecurity professionals can learn more about the implications of any security initiatives on business operations. For instance, some companies are deploying a talent-factory model that encourages cybersecurity professionals to work in other areas of the company in short rotations to broaden their perspectives. Their assignments may be focused on learning more about technology topics outside the security area—for instance, network management, core IT infrastructure, and application development. In an ideal world, cybersecurity team members would be embedded in business units to learn more about product management, public affairs and communications, or finance. The result is often more knowledge sharing and better communication among teams.

The cybersecurity and IT groups should use all available tools and technologies at their disposal to learn as much as they can about people and processes, thereby creating more transparency about security issues. They should establish clear policies outlining which employees at which levels can call up which categories of data, and when. Where permissible, they can back up these policies with a comprehensive identity-and-access management system—a rules-based platform that automatically monitors online activities, approves access rights, and issues alerts. Additionally, where permissible, they may use predictive analytics to identify risks before breaches can occur—for instance, using network information and log-in data to identify potentially malicious actors and activities inside the company.

Trust gap 3: The company and its vendors

The relationship between companies and their technology and supply-chain vendors has always been complex. Just as consumers rely on companies to keep their data safe and to use them only in ways that they have authorized, businesses must trust their IT and supply-chain vendors to hold competitive information close to the vest. Automakers, for instance, would need to be confident that their OEMs have enough cybersecurity controls in place to protect the intellectual property they are sharing.

This is especially true in an era in which more and more companies are outsourcing the management of their IT infrastructures or their cybersecurity operations. Businesses need to be assured that the access they provide to vendors and the offerings they get from vendors can be integrated with existing systems without opening up any security holes.

Bringing partners closer

To bridge this trust gap, company IT and business leaders should schedule regular conversations with vendors and supply-chain partners to assert the levels of security required to protect shared business information. Such meetings should take place quarterly or biannually; with more frequent contact, vendors and company officials can engage in a true business partnership rather than a simple transactional relationship. They can discuss and devise clear recovery and compensation plans.

Companies can take it a step further by actively collaborating with third-party providers and supply-chain partners to ensure sufficient data protection. They may jointly pursue security certifications, such as the Payment Card Industry Data Security Standard or the ISO 27001 standard, or conduct joint reviews and security audits of IT systems. They may even agree to open themselves up to a broader ecosystem of technology partners to provide additional checks and balances.

For their part, technology vendors may include conditions in their service-level agreements, for instance, for recovering data or restoring system availability within designated time frames. Or they may agree to provide insurance to cover any business the company loses as a result of an attack on the vendor's systems. Many insurance companies are beginning to incorporate cyberincidents into their actuarial tables. The typical coverage today is still narrow, but these policies may become another tool vendors and supply-chain partners can use to assure companies that they are being protected against cyberattack—thereby closing the trust gap.

Trust gap 4: The company and the government

It's no surprise that local, national, and federal governments have in recent years prompted private-sector organizations to become more aware of cybersecurity issues and more active in their data-protection efforts. Cyberattacks in major financial institutions can affect overall market stability. Energy-grid hacks can pose

How agile development can help close the trust gap between the business and IT

It’s worth noting that, often, the cybersecurity trust gap between IT and the business units can spill over into product development, particularly in companies that provide online services and Internet of Things solutions. The business units want to establish feature-rich websites and mobile channels that facilitate the customer purchasing experience. Meanwhile, the IT and cybersecurity teams are compelled to introduce security protocols to ensure not only that customer data are protected but that company systems are not left open to attack. And such protocols are not always in sync with the business units’ desire to create convenient paths for customers. The result is a lack of shared understanding and a strong sense of frustration—on the part of the business leaders, who view IT as an obstacle to innovation, and on the part of technology leaders, who view the business units’ desire for unfettered experimentation as a critical cybersecurity risk.

Companies could instead explore agile approaches to product development—allowing cybersecurity experts to work alongside product owners from the business units as well as colleagues from across multiple functional areas. In this way, companies can establish a collaborative environment that breaks down silos between the IT organization, the cybersecurity team, and the business units. Under this approach, data-protection protocols can be factored into product designs at the outset, reducing potential conflicts or the need for system patches or rework later in the development process.

national threats, too, as we learned from the recent attempted break-ins at a dozen power plants in the United States. Government agencies need companies to report cyberattacks and other incidents in a timely fashion, in order to strengthen overarching protection efforts—for instance, spotting and addressing suspicious patterns of activity and alerting the public to any dangers.

Seeing the big picture

Neither side can afford to battle cyberattacks on its own. Companies need the official imprimatur and gravitas that government agencies can provide as facilitators of cybersecurity investigations and discussions of sensitive information. Governments need the feedback and technical resources that private-sector organizations can provide.

Across the globe, governments are taking steps to support businesses’ improvements to their cybersecurity programs. The government of Australia hosts annual cybersecurity leadership meetings, where the prime minister and business leaders set strategy for bolstering cybersecurity efforts in both the private and public sectors. And the government of Singapore has also launched a series of public- and private-sector collaborations designed to strengthen the country’s capabilities in cybersecurity research.

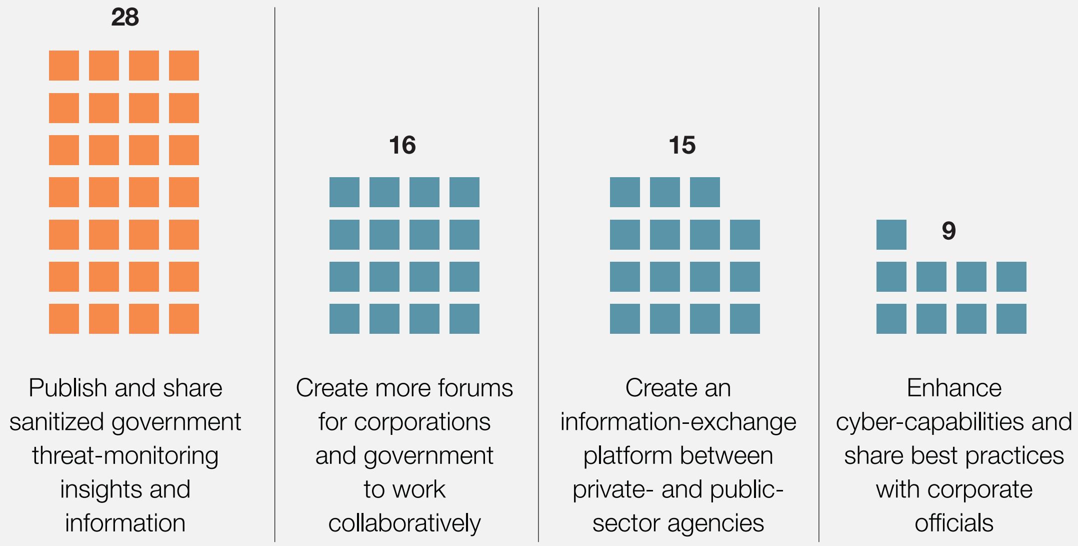
For their part, some companies believe there are ways to further improve public-private partnerships (Exhibit 3). One chief information security officer at a global bank cited the need to extend the national detection network. A CIO at a financial-services company advocated for increased sharing of actionable intelligence. “So far, there are only a few forums aimed at specific corporations. It’s not enough for most companies,” he told us.

◆◆◆

EXHIBIT 3

Companies and government agencies must improve how they share security-oriented information.

Q. What should the government do to improve information sharing?, number of times suggested by executives



Source: Insights derived from interviews with about 270 chief information security officers and other top executives at the World Economic Forum; McKinsey analysis.

Technology alone cannot hold cyberattackers at bay. A culture of trust is also important for corporate cybersecurity initiatives to succeed. All stakeholders in a company's ecosystem—board directors, IT leaders, businesspeople, vendors, and so on—must come to a mutual understanding of the risks the company faces and work together to decide on the best approach for addressing those risks.

As we've learned, it can be difficult to attain and preserve this level of agreement and trust—particularly because of the natural tensions built into data-protection efforts: the cybersecurity team's day-to-day work has consequences for the business and vice versa. But if companies recognize the human aspect in cybersecurity and take steps to close trust gaps by introducing more transparency, they can increase the odds that their cybersecurity programs will be successful—not just in the near term, but over the long haul, regardless of the kinds of threats that may emerge. ◆

Jason Choi is a consultant in McKinsey's Hong Kong office, where **Harrison Lung** is an associate partner; **James Kaplan** is a partner in the New York office.

The authors wish to thank Tom Barkin, Chandru Krishnamurthy, Suneet Pahwa, Chris Rezek, and Paul Willmott for their contributions to this article.

Digital/McKinsey

November 2017
Designed by Global Editorial Services

McKinsey.com
@DigitalMcKinsey
facebook.com/DigitalMcKinsey