ANDREW BECKETT

Managing Director, EMEA Head
Cyber Risk
London, UK
andrew.beckett@kroll.com

BENEDETTO DEMONTE

Managing Director, North America Head
Cyber Risk
New York, NY, US
bdemonte@kroll.com

PAUL JACKSON

Managing Director,
Asia Pacific Head
Cyber Risk
Hong Kong, China
paul.jackson@kroll.com

JASON SMOLANOFF

Senior Managing Director, Global Head
Cyber Risk
Los Angeles, CA, US
jason.smolanoff@kroll.com

Cybersecurity Breaks Out of Its Silo

Cyber intrusions can quickly morph into legal, financial and reputational crises. To keep pace, cybersecurity is transcending its traditional boundaries.

In a world in which digital assets can be more valuable than physical assets, and computer networks control operations from production to customer service, cybersecurity can no longer be seen as a stand-alone function. Instead, it is now part of a larger security picture, just as cybercrime is now simply crime pursued by digital means rather than some narrow form of technical malfeasance. This trend is highlighted in our survey results, which show that across a range of incident types, computer networks were the primary channel of the intrusion in one-fifth to almost one-half of cases. But even for incident types where cybersecurity breaches are most likely to be a primary cause—such as data or IP theft—plenty of cases exist in which cyber breaches played only a partial or even little to no role. The traditional silo around cybersecurity, like so many other silos today, is breaking down (see Figure 18 on page 62).

> Companies that spend millions of dollars on technology solutions must ensure that they also provide the ongoing resources, policies and procedures needed to make that technology work.

MOVING BEYOND THE ARMS RACE

This convergence of risk is bringing about a new way of thinking about cybersecurity and **who in the organization is responsible for it**. It is increasingly common, for example, for organizations to charge either the general counsel or a chief security officer with overseeing the entire risk portfolio, including cybersecurity. The chief information security officer thus becomes part of a team of executives whose collective remit might include physical security, threat assessment, crisis management and more.

Risk convergence is also leading organizations to adopt a broader strategy to **cyber risk assessment**. Traditionally, cybersecurity has been approached as a technology-driven arms race against bad actors. Today, however, forward-thinking enterprises set cybersecurity priorities by looking inward to identify the most important elements of the business and the data and technologies those elements involve. This examination is followed by a deceptively simple question: Exactly why do we need a cybersecurity program? For example, a freight company might see cybersecurity as a means of meeting insurance requirements, whereas a bank may consider cybersecurity a key element of its brand promise.

Placing cybersecurity within the organization's larger strategic picture also sheds light on the types of **threat actors** that an organization faces, because different threat actors gravitate toward different assets. Organized crime, for example, typically targets payment processors. State-sponsored hackers, by contrast, prefer intelligence gleaned from airline passenger itineraries. Each category of actor will have its own characteristic set of behaviors and tools to be countered. This more holistic view of the cyber threats a company faces allows it to better determine what steps will bring its cybersecurity risk below its risk appetite threshold.

Just as organizations are taking a broader view of their cyber risk, so too are they taking more sophisticated approaches to **risk mitigation**. The continual emergence of new risk vectors means that serious intrusions are no longer a question of *if* but *when*. As a result, cyber strategy is no longer dominated by protection; organizations are working to distribute attention among identification, protection, detection, response and recovery. Doing so requires the coordination of multiple aspects of the organization, including the business, compliance, communications, internal audit and legal departments.

Implementing this broader approach calls for a greater understanding across the organization of what is required and what is at stake. An organization's cybersecurity leaders no longer make the mistake of thinking that issuing a policy is the same as enforcing one; they also have more sensitivity to the cost in time and convenience that cybersecurity requirements impose across the enterprise. In turn, the rest of the business increasingly understands its role in preventing cyber breaches and the very real impact those incidents can have.

WHY CYBERSECURITY FAILS

Even a comprehensive and well-designed cyber program, however, can fall short in its implementation. Indeed, most cyber breaches occur not because of a lack of design but rather because of poor execution. The ability to execute depends on the **operational maturity** of an organization's cyber measures—that is, how well those measures are supported by other aspects of the business. A first-class cyber threat detection system, for example, is of little use without an adequate number of trained personnel who can respond quickly to the alerts generated by that system. A commitment to remediate the harm done to customers who have had their account records stolen needs to be backed up with customer service centers that can quickly scale to handle the influx of calls certain to occur after an incident.

It is ironic that operational maturity is of such importance to cybersecurity yet so often gets little attention. Companies that spend millions of dollars on technology solutions must ensure that they also provide the ongoing resources, policies and procedures needed to make that technology work.

REACHING OPERATIONAL MATURITY

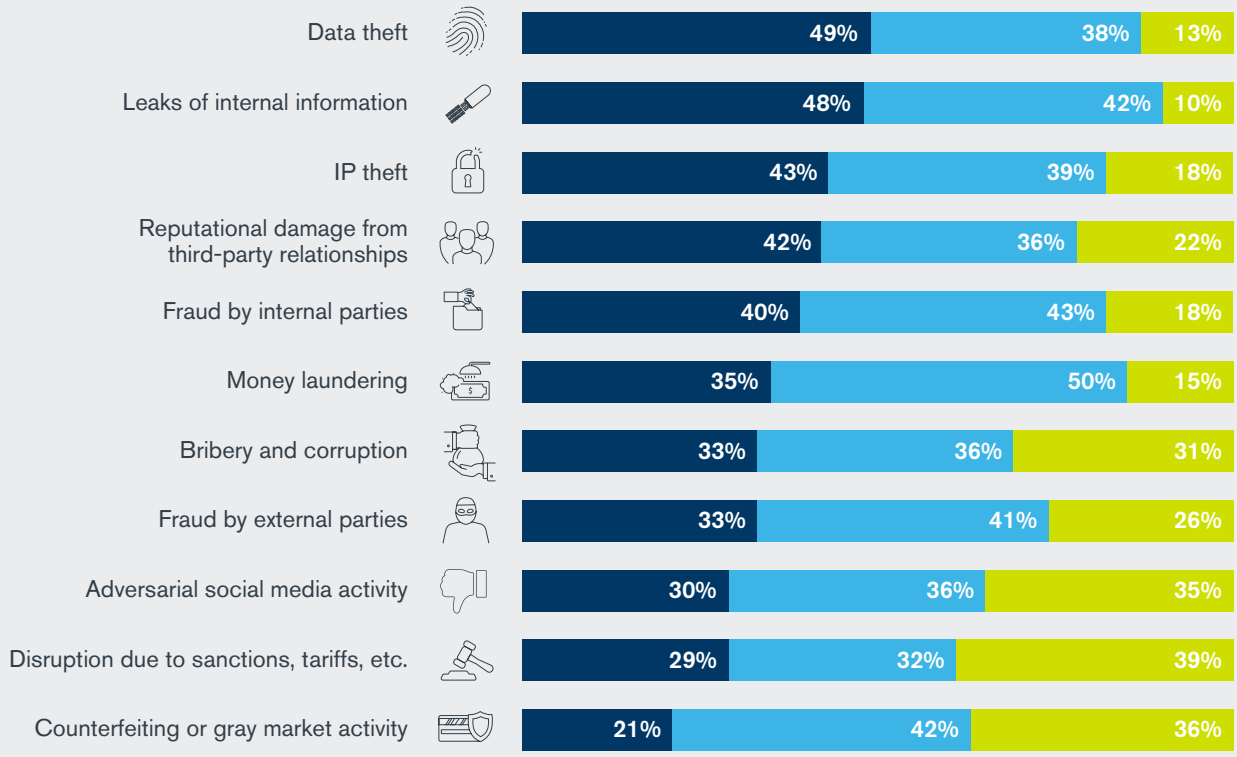
Organizations can take two important steps to accelerate their operational maturity. The first is to have adequate **strategic and tactical governance**. This helps ensure that a holistic cyber strategy has been developed, sufficient resources have been allocated and the necessary processes and procedures have been put in place. At a tactical level, good governance provides the mechanisms for resolving conflicts between policy and implementation that come about even when everyone involved is sensitive to the costs and necessity of cybersecurity compliance. Further, conflicts arise between various aspects of security. Network security and information security, for example, have different approaches and priorities, frequently requiring mediation between the two.

Second, organizations need to establish the sufficient **internal audit and control capabilities** to monitor the performance of their cybersecurity systems as well as the elements, like the security operations center, that support it. To the extent possible, that auditing should involve quantitative measures of performance rather than merely subjective assessments. Real-time monitoring should be complemented with tabletop exercises that test the responses of people and systems under more extreme conditions.

Cybersecurity poses systemic challenges to many organizations: Its boundaries shift constantly, it requires ongoing commitment and it doesn't directly generate revenue. Yet it does help create trust and confidence, which are both essential for revenue-generating relationships. Furthermore, now that cyber issues are so deeply woven into the fabric of most businesses, expanding an organization's cybersecurity efforts will significantly mitigate risks throughout the enterprise.

FIGURE 18

WHAT ROLE DID COMPUTER SYSTEM BREACHES PLAY IN INCIDENTS DURING THE LAST YEAR?*



*"Don't know/Not applicable" responses excluded. Percentages do not total 100 percent due to rounding.