COMBATING CYBER RISK

HOW TO ATTACK A GROWING THREAT

RAJ BECTOR
DAVID X MARTIN

Advances in electronic connectivity and data storage have made the exchange of large quantities of information, even over vast distances, cheaper and quicker than anyone could have imagined possible 30 years ago. The gains in efficiency to businesses and benefits to consumers have been extraordinary.

However, opportunities for crime have also expanded. The new informational openness on the part of enterprises is being used to subvert their operations and to steal their intellectual property and the "identities" of their customers.

The losses can be large – be they in the form of compensation to customers, disruption of business, reputational damage, or, even, in the payment of ransom to have "captured data" from computer systems returned. Since 2010, the number of registered cyberattacks around the world has been growing at a rate of 23 percent per annum and now stands at 116 every day. The average annual cost of cyberattacks to affected businesses is $9 million.

The natural response to the threat of defense is to erect barriers: high walls and moats, with drawbridges that are lowered only for clearly identified "friends." This has been the traditional approach to cybersecurity. Access was granted only to users and computers meeting narrowly defined specifications and able to pass rigorous identity tests.

But this old-fashioned line of defense is untenable today. The business models of many firms now depend on their computer systems and data being open to thousands or even millions of other computers, potentially anywhere in the world. Making it difficult for outsiders to "get in" – to send you emails or search your site or buy something from it – is not an option. Customers would rapidly defect to competitors who made access easy.

Instead, firms must learn to manage cyber risk while keeping their borders open. For most firms, cyber risk is an unavoidable part of doing business, in the way that credit risk is a natural part of the banking business. They must manage cyber risk in the same way that they manage more familiar operational risks.

A QUANTITATIVE APPROACH

The first step to implementing this new methodology is to put a price on cyber risk. If you don't know what something costs, you can't know if it is worth the benefits it delivers or how much it is worth spending to reduce it.

Firms can now insure themselves against cyberattacks. The premiums provide firms with a cost for the cyber risk they are taking. When evaluating the returns of any product, line of business, or proposed venture, such premiums should be added to the accounting. If an apparently profitable venture becomes unprofitable once these insurance premiums and other items are added, then it may not be worth the risk it entails.

Cyber risk mitigation efforts can be valued in the same way. A new cybersecurity feature is worthwhile only if it costs less than the net present value of the resulting reduction in cybersecurity insurance premiums.

This logic applies even when the cyber risks aren't insured, either because insurance is unavailable or because the firm prefers to self-insure by holding capital against these risks. If the cost of the required capital tips a venture into the red, then it entails too much risk.

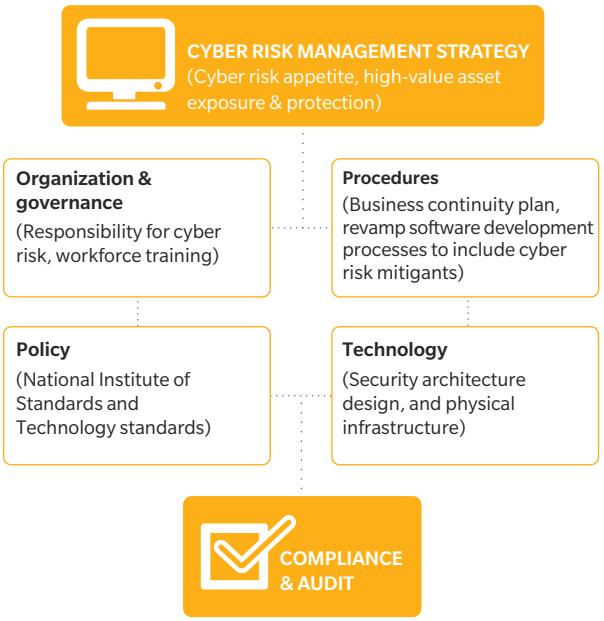
Putting a monetary value on cyber risks is difficult for the same reason that it is problematic for many operational risks. Because the serious risks – the causes of very large losses – are such rare events, their probability cannot be determined from historic data. Moreover, an operational risk event, such as a cyberattack or internal fraud at a bank, changes the probability of other such events. People now know that it can be done. This encourages both copycatting and preventative measures.

For this reason, many operational risks, including cyber risks, are best evaluated using scenario analysis rather than historical data. In this case, cybersecurity experts work with commercial managers to estimate the likelihood of various kinds of attacks and how much they would cost the enterprise.

Though not based directly on historic data, this approach is informed by it. For example, estimates of losses from attacks that would require market notification can be guided by the observed devaluations of firms that have made such notifications. And cyber risk experts will be directed by information about the frequency of various kinds of attacks occurring around the world.

Scenario analysis not only helps to quantify the risk. It also helps to reduce it. Most importantly, it assists firms with identifying "tripwires" – events which signal to the

EXHIBIT 1: AN ENTERPRISE-WIDE CYBER RISK MANAGEMENT FRAMEWORK



- An overarching **cyber risk strategy** is created, based on risk appetite, environment, and capabilities
- **Governance** structures are installed to control cyber risk and security throughout the organization
- **Security policies** are derived to bring the cyber risk strategy and compliance up to industry standards (PCI, ISO, FISMA)
- **Suitable personnel** are selected and trained. Risk culture is established
- **Security processes** are aligned to the cybersecurity strategy and security policies (war gaming, threat modeling, access control, background screening, secure development, pen testing, business continuity)
- **Technology infrastructure** is deployed to support security processes (information security architecture, systems integrity, monitoring/detection tools, network redundancy)
- **Physical infrastructure** is designed and installed with access controls, surveillance, and crisis management to provide a secure foundation for processes and IT infrastructure
- **Regular audits** are conducted to ensure compliance and performance with defined processes

Source: Oliver Wyman analysis

firm that it may be under attack and trigger preventative action. Law enforcement agencies often employ these techniques to counter terrorist attacks. Precursor actions, such as the purchase of certain chemicals are identified for a given incident. When potential criminals take those actions, they set off the tripwire, alerting authorities.

116

The number of registered cyberattacks around the world every day

CONTAINING CYBER RISK ACROSS AN ENTERPRISE

How much cyber risk should firms accept, and how much resources should be expended toward its mitigation? These are strategic issues that require input not just from the information technology department but also from risk, finance, business lines, and ultimately, the company's chief executive officer and board of directors. Again, there is nothing unusual about this. It's how operational risks are normally addressed.

Some firms recognize the enterprise-wide significance of cybersecurity. (See Exhibit 1.) And regulatory initiatives such as the National Institute of Standards and Technology are forcing executives outside the IT department to pay attention. Nevertheless, few firms have yet to establish an enterprise-wide framework for managing cyber risk.

Cyber risk poses entirely new challenges to firms. Yet the key to managing it is recognizing that it is simply a new variant of a familiar problem. Cyber risk is just another operational risk. The approaches to measuring and managing operational risk that have been developed over recent decades can be applied to cybersecurity.

Of course, cyber risk involves a level of complexity and a pace of change that exceed most other operational risks. As a result, new skills and some dedicated staff are required. But this does not mean that cybersecurity must be left to these specialists. It is a job for the entire enterprise, starting with leadership from the senior management team.

Raj Bector is a New York-based partner in Oliver Wyman's Strategic IT & Operations practice.
David X Martin is a member of the Oliver Wyman Senior Advisory Board, special counselor to the Center of Financial Stability, adjunct professor at New York University and author of *The Nature of Risk*.