OLIVER WYMAN

Financial Services

POINT OF VIEW

A NEW APPROACH TO CYBERSECURITY

LEVERAGING TRADITIONAL RISK MANAGEMENT METHODS

AUTHORS

David X Martin
Senior Advisory Board Member

Raj Bector
Partner

MARSH & McLENNAN COMPANIES

1. INTRODUCTION

Businesses must exchange information with many different external bodies from current and prospective customers and suppliers, to government agencies and joint venture partners. This communication was once slow and expensive for both parties, especially when they were far apart.

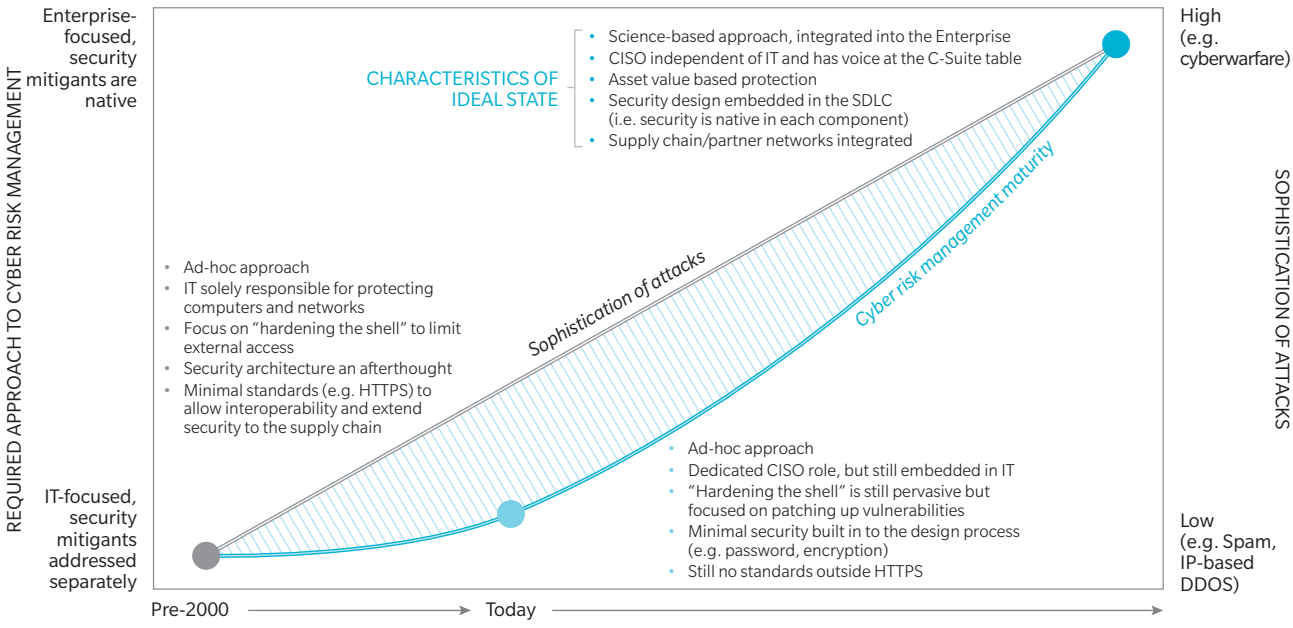
Not now. Advances in electronic connectivity and data storage have made the exchange of large quantities of information, even over vast distances, cheaper and quicker than almost anyone imagined possible even 30 years ago.

The efficiency gains and benefits to consumers are extraordinary. However, the explosion of data and interconnectedness has also expanded the opportunities for crime. The new informational openness of enterprises is being used to steal their intellectual property, the "identities" of their customers and to subvert or shut down their operations. In recent years, the sophistication of cyberattacks has increased exponentially, while the defensive approach has largely remained the same (see Exhibit 1).

The losses from cyberattacks can be large – be they through compensation to impacted customers, disruption of business, reputational damage or, even, paying ransoms to have "captured data" from computer systems released. Since 2010, the number of registered cyberattacks around the world has been growing at a rate of 23% per annum and now stands at 116 every day.[1] The average annual cost of cyberattacks to affected businesses has grown 17% per annum to reach $9 MM.[2] As the informational openness of businesses and the creativity of cybercriminals continues to grow, so does this cyberthreat.

The established approach to cybersecurity has become untenable. In the new age of online communication and transacting, putting a "hard shell" around the enterprise will cost more in lost business or inflated transaction

Exhibit 1: Old vs. new approach to cyber risk (Illustrative)



1-2 Source: Symantec Internet Security Threat report; Ponemon 2012, 2013 Costs of Cyber Crime study; The Global State of Information Security® Survey 2014; The Betterly Report Cyber/Privacy Insurance market survey 2013; Cybersecurity Market report by Marketsandmarkets, June 2012.

costs than it saves in reduced losses from cyberattacks. Businesses must instead approach cybersecurity as they (should) approach other risks entailed by their business activities.

As we explain in this Oliver Wyman Point of View, that means taking a science-based approach to cyber risk management, quantifying the cost of cyber risk, taking a cost-benefit approach to risk mitigation and factoring cyber risk into strategic decisions. In other words, cyber risk must become an issue not just for the IT department but for Risk, Finance, business heads, and, indeed, for the CEO and the Board.

2. CYBER RISK CANNOT BE ELIMINATED

The natural response to the threat of attack is to erect barriers: high walls, moats and 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 basic identity tests.

This approach is untenable today. The business model of many firms now depends on their computers, networks, and select 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 more easy. In short, the cost in lost business would greatly exceed the savings in reduced losses from cyberattacks.

Firms must learn to manage cyber risk while keeping their borders open. For most firms, cyber risk is just an unavoidable part of doing business, in the way that credit risk is a natural part of the banking business. It is something that cannot be eliminated and must be managed.

This makes cyber risk a strategic issue. Senior managers, and not just the Head of IT, must decide which products, lines of business or ventures are worth the cyber risk they entail. And they must decide how much it is worth spending to reduce cyber risks.

This requires someone in the firm to understand the different kinds of cyberthreats and where they are most likely to strike. But it also requires a way of putting 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. This experience lives with risk managers; they have the tools, methods, and techniques to manage cyber risk as a science.

3. A QUANTITATIVE APPROACH

Firms can now insure themselves against cyberattacks. The premiums of insurance policies 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 and financial impact from reputational risk, potential loss of revenue, etc. should be added to the accounting. If an apparently profitable venture becomes unprofitable once these insurance premiums and other items are added, then it is not worth the cyber risk it entails.

Cyber risk mitigation efforts can be valued in the same way. If a new cybersecurity feature costs less than the net present value (NPV) of the resulting reduction in cybersecurity insurance premiums, then it is worthwhile. If it costs more, it may not be.

This logic applies even when the firm carries no applicable cybersecurity insurance, either because it is unavailable or because the firm prefers to self-insure by holding capital against the risks (as for Banks holding regulatory capital for losses due to operational risk). If the cost of the required capital tips a venture into the red, then it entails too much cyber risk. Or if the NPV of the cost of the capital saved by a risk mitigation initiative is less than cost of the initiative, then it is better to live with the risk.

In other words, cyber risk should be dealt with in the same way that other operational risks are. Not just in the way it contributes to decision-making but in the way it is measured (see Section 4) and in the way governance is placed around it (see Section 5).

We have developed two approaches to quantifying cyber risk:

1. Asset-based approach: Quantify the value of corporate assets (e.g. data, services) plus the brand/reputational damage that could materialize from a cyberattack. Use probability of a threat becoming a reality (similar to probability of default in banking credit risk terms) and expected loss of value of corporate assets (similar to expected loss).
2. Liability-based approach: What is the liability to the business if a threat were to materialize? This requires playing out various business-oriented scenarios and anticipating and quantifying the financial and reputational loss. This method typically relies on past loss event data to estimate liability, which can lead to imperfect results.

4. SCENARIO ANALYSIS

Irrespective of the quantative approach used, putting a monetary value on cyber risks is difficult, and for the same reason that it is difficult for many operational risks. The serious risks – the causes of very large losses – are rare events. This means that their probability cannot be determined from historic data. Suppose that, in the last 5 years, there has been just one cyberattack causing a loss in excess of $100 MM in a universe of 1,000 firms that might suffer such an attack. It does not follow that probability of a cyberloss in excess of $100 MM is 0.02%. For all such a single data point tells you, the chance could be anywhere between 0% and 100%.

The occurrence of an operational risk event, such as a successful cyberattack or internal fraud at a bank, does not merely provide information about the prior probability of such an event, it changes the probability. People now know that it can be done. This encourages copycatting and also preventative measures. At the extremes, this can push the probability of repeats of the event in question to 100% or 0%. Even without such implausibly dramatic effects, any information that the event provides about the (prior) likelihood of such events is sure to be overturned by the way its occurrence changes people's behavior.

For this reason, many operational risks, including cyber risks, are best evaluated using scenario analysis in conjunction with historical data. Under this approach, cybersecurity quantitative experts (i.e. cyber risk experts) work with commercial managers to estimate the likelihood of various kinds of attack 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 in the past. And the cyber risk experts will be guided by information about the frequency of various kinds of attacks occurring around the world. By pooling information about the cyberattacks they experience, firms and their insurers can improve the quality of their scenario analysis.

Scenario analysis does not only help to quantify the risk; it helps to reduce it. Most importantly, it helps firms to identify "tripwires" – events which signal to the 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 make those actions, they trip the wire to alert the authorities.

5. CYBER RISK MANAGEMENT IS AN ENTERPRISE-WIDE JOB

Deciding how much cyber risk to accept, how much to spend mitigating it, and where to accept and mitigate it, are issues that require a strategic view. They require input not just from the IT department but from Risk, Finance, the business lines and, ultimately, the CEO and the Board. Again, there is nothing unusual about this; it's how things usually are with operational risks.

Exhibit 2: 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 fulfill the cyber risk strategy and compliance to industry standards (PCI, ISO, FISMA, etc.)
- Selection of **suitable personnel** and their training in the processes are designed. 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 the 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 ensure compliance and performance with defined processes, policies across all three dimensions

Some firms have recognized the enterprise-wide significance of cybersecurity. And regulatory initiatives such as the National Institute of Standards and Technology (NIST) have forced executives outside the IT department to start thinking about cybersecurity. Nevertheless, few firms have yet established an enterprise-wide framework for managing cybersecurity.

Getting cybersecurity right needs involvement from all parts of an enterprise (see Exhibit 2):

- Enterprise Risk Management, IT and Compliance jointly need to make sure that the cyber risks are pinpointed throughout the firm, that they are properly mitigated and that, when things go wrong, lessons are learned and communicated
- Compliance must make sure that processes and systems comply with privacy and data protection laws and internal control measures
- Business Continuity must plan for a higher degree of resiliency, and extend disaster recovery to non-physical damage
- Finance needs to consider developing the accounting framework for cyber risk and decide whether to transfer (some of) that risk using insurance. There could be a "cyber risk charge" for business lines that expose the firm to excessive cyber risk.
- Legal needs to consider regulation, litigation possibilities, contractual obligations, and the firm's ability to provide evidence to third parties of proper data protection processes
- Business line management needs to ensure that the control framework, including standards and guidelines, is actually in place

Cybersecurity poses firms with entirely new challenges. Yet the key to managing cyber risk is recognizing that it is merely a new variant of a familiar problem. Cyber risk is simply another kind of 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. And this requires new skills and some dedicated staff. But this does not mean that cybersecurity can be left to these specialists. It is a job for the entire enterprise, starting with the Board and the CEO.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

ABOUT THE AUTHORS

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. He is a former Chief Risk Officer and founding chair of the Investment Company Institute's Risk Committee.

Raj Bector is a Partner at Oliver Wyman with extensive experience in risk management in Financial Services operations and technology and has significant experience supporting institutions with anticipating and analyzing cybersecurity threats.

www.oliverwyman.com

OLIVER WYMAN