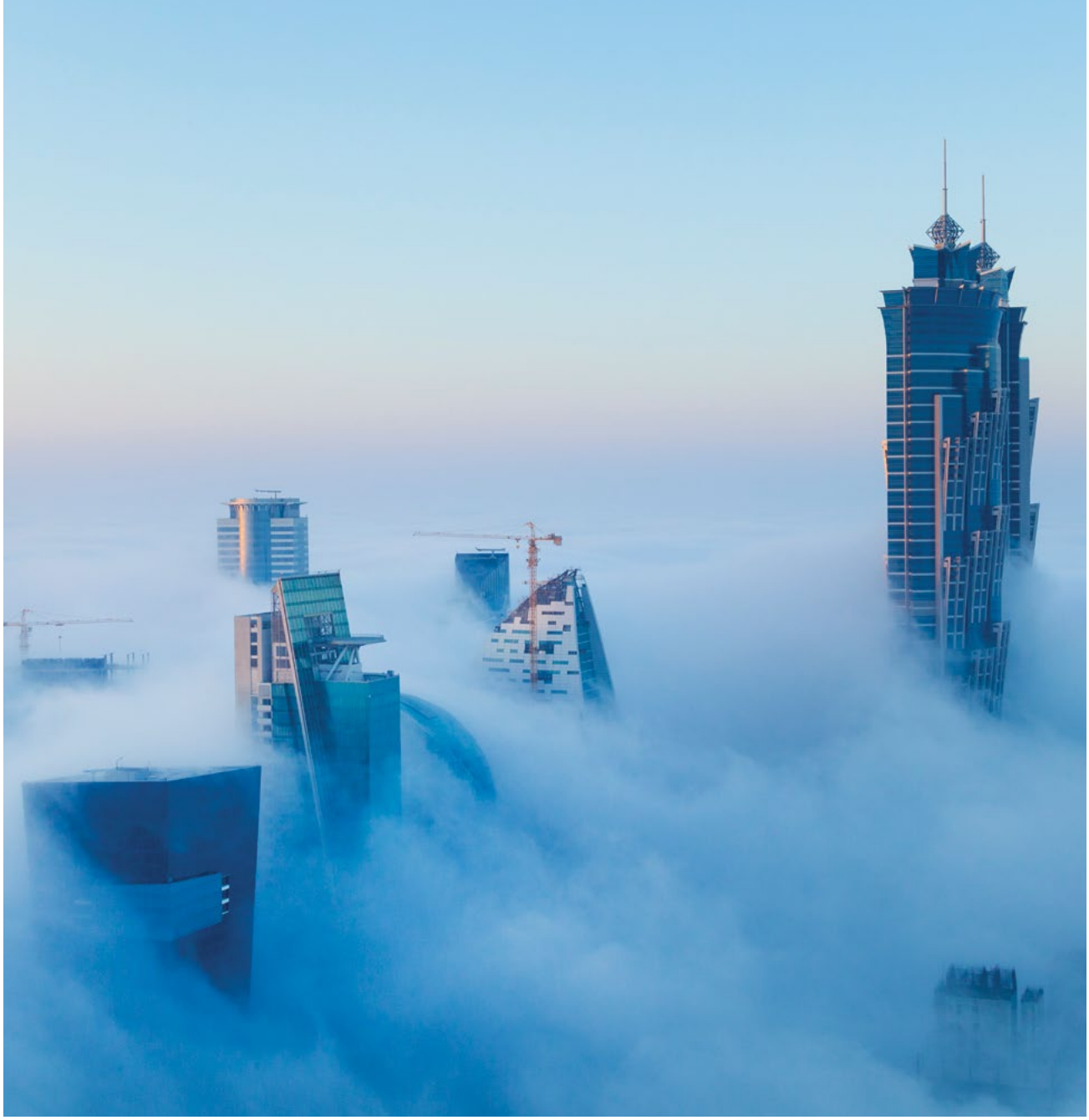

QUANTIFYING CYBER RISKS

CAN YOU PUT A DOLLAR AMOUNT ON YOUR COMPANY'S CYBER RISK?

Leslie Chacko • Claus Herbolzheimer • Evan Sekeris

Cyber breaches are one of the most likely and most expensive threats to corporations. Yet few companies can quantify just how great their cyber risk exposure truly is, preventing them from effectively protecting themselves.

Most managers rely on qualitative guidance from "heat maps" that describe their vulnerability as "low" or "high" based on vague estimates that lump together frequent small losses and rare large losses. But this approach doesn't help managers understand if they have a $10 million problem or a $100 million one, let alone whether they should invest in malware defenses or email protection. As a result, companies continue to misjudge which cybersecurity capabilities they should prioritize and often obtain insufficient cybersecurity insurance protection.

No institution has the resources to completely eliminate cyber risks. That means helping businesses make the right strategic choices regarding which threats to mitigate is all the more important. But right now, these decisions are made based on an incomplete understanding of the cost of the various vulnerabilities. Organizations often fail to take into account all of the possible repercussions, and have a weak grasp of how the investments in controls will decrease the probability of a threat. It's often unclear whether they are stopping a threat or just decreasing its probability – and if so, by how much?

It's essential that companies develop the capability to quantify their cyber risk exposure in order to form strategies to mitigate that risk. The question is, is it really possible to put a dollar sign on fast-changing cyber risks with data that is difficult to find and often even harder to interpret?

CONSIDER A BROADER SET OF LOSSES

Estimating the true cost of a potential cyber breach may never become an exact science. The good news is that our understanding of why cyber risk forecasts keep falling short is improving. The main culprit is that companies quantify cyber risks the same way they do other operational risks – focusing narrowly on potential direct revenue losses. But companies can make much more accurate forecasts if they evaluate cyber risks on a broader set of losses associated with cyberattacks.

Companies come much closer to properly weighing how much they should spend to reduce their cyber risk and curb cybercrime when they consider these risks from three perspectives – foregone revenue and ancillary payments, liability losses, and reputational damage. One reason for this is that they are able to capture one of the biggest differences between cyber threats and other risks to their business: Cyberattacks can hurt a company even if there is no gain for the perpetrator other than accessing sensitive information.

The direct revenue losses for the companies involved in a cyberattack can be nearly negligible compared to the reputational damage incurred, which in turn can lead to future revenue losses. That is why it is essential for managers to quantify cyber risks more broadly. It can be done, and can potentially save companies hundreds of billions of dollars every year.

EXHIBIT 1: THE STATE OF CYBER RISK MANAGEMENT AT A GLANCE

COMPANIES STILL DO NOT DEVOTE SUFFICIENT RESOURCES TO CYBER RISK MANAGEMENT

77%
of corporations do not assess their suppliers or customers for cyber risk

68%
of corporations have not estimated the financial impact of a cyberattack

43%
of corporations have not yet identified one or more cyber scenarios that could affect them

30%
of corporations have less than a basic understanding of their cyber risk exposure

25%
of corporations do not include cyber risks in their corporate risk registers

Source: European 2015 Cyber Risk Survey Report, Marsh, Global Risks 2015, medium and large-size corporations

IDENTIFY THE GREATEST VULNERABILITIES

The first step in putting a dollar figure on cyber risks is to identify your company's most important assets and its greatest vulnerabilities. Cyber risks generally fall into two categories: 1) those involving services shutting down, and 2) those that compromise information, ranging from sensitive data, to corporate secrets, to bank accounts.

But assumptions differ greatly, depending on a business and its customers. For example, a utility company's greatest cyber risk could be a nuclear plant outage, while a health insurer's top cyber risk may be losing medical data or having a hacker unexpectedly cripple critical surgical equipment. For another business, the greatest cyber risk could be the abrupt inability to bill customers, or perhaps, in the case of a bank, a shutdown that prevents customers from getting paid.

The challenge then is to build a smart, well-designed, cyber risk model that's able to analyze potential direct revenue, liability, and brand loss scenarios. For when a cyberattack happens, companies are hit not just with losses resulting from customers who stop buying products and services; they also face ancillary costs related to fixing their problem, such as regulatory fines, forensics, and consulting costs.

Liability losses, too, come into play in cases where critical data is accessed. A company may need to provide customers years of remediation, such as offering credit monitoring services, along with legal fees and penalties to settle multiple class-action lawsuits. Finally, companies must quantify how much their future revenues will fall if a cyberattack has damaged their brand.

DEFINE THE UPPER AND LOWER RISK BOUNDARIES

To understand the upper and lower boundaries of their risk, companies must gather general business, operational, and technical data that can be modeled against expected and worst case scenarios. Using both internal and external data related to the health of their business and operations, managers should be able to predict their expected and maximum cyber losses over a one- to three-year period, just as they can forecast their future revenues. They can also estimate what percentage of their future customers will leave if an outage results from a cyber breach – or how much their stock valuation and margins could suffer if a cyberattack taints their reputation. Companies should also judge, in part from past incidents, which applications are at the highest risk.

Armed with this information, it's much easier for managers to judge if their companies have the right level of cyber risk protection and to budget for potential additional spending. Answers to questions like how much the company should invest in evaluating the state of their vendors' cybersecurity become much clearer. Or at what cost more authentication software is appropriate, given the likelihood that critical data will be accessed.

Managers can also weigh if they should invest in more training of employees and vendors or in more technical controls to monitor potential cyber breaches. In some cases, managers may even discover that investing in a new product line may, or may not, be worthwhile given the cyber risks involved.

Quantifying cyber risks is challenging – but feasible

Quantifying cyber risks is challenging, but feasible – and you can't afford not to do it. Most firms have the technical knowhow and a strong enough grasp of the risks involved to help managers evaluate the trade-offs involved in mitigating cyber risks with a much smaller margin for error than in the past. What's needed now is leadership from managers to prioritize the need to gain a better understanding of how much to spend to curb cyber risks and put a halt to cybercrime.

Leslie Chacko is a San Francisco-based principal and **Claus Herbolzheimer** is a Berlin-based partner in Oliver Wyman's Digital and Strategic IT practices. **Evan Sekeris** is a Washington, DC-based partner in Oliver Wyman's Financial Services practice.

This article first appeared in Harvard Business Review.