10 GO TO CYBER EXTREMES

What to do when digitalization goes wrong

Claus Herbolzheimer

For years, conventional wisdom has dictated that organizations focus on preventing the most common types of cyber-attacks, rather than preparing for that one all-encompassing disaster that might never occur. But in reality, it is no longer possible to make such a tradeoff. Full-blown cyber crises – some of them life-threatening – are becoming more common. Increasing digitalization and interconnectedness are exposing organizations more frequently to more sophisticated kinds of cyber threats. Planning for worst-case scenarios is no longer optional.

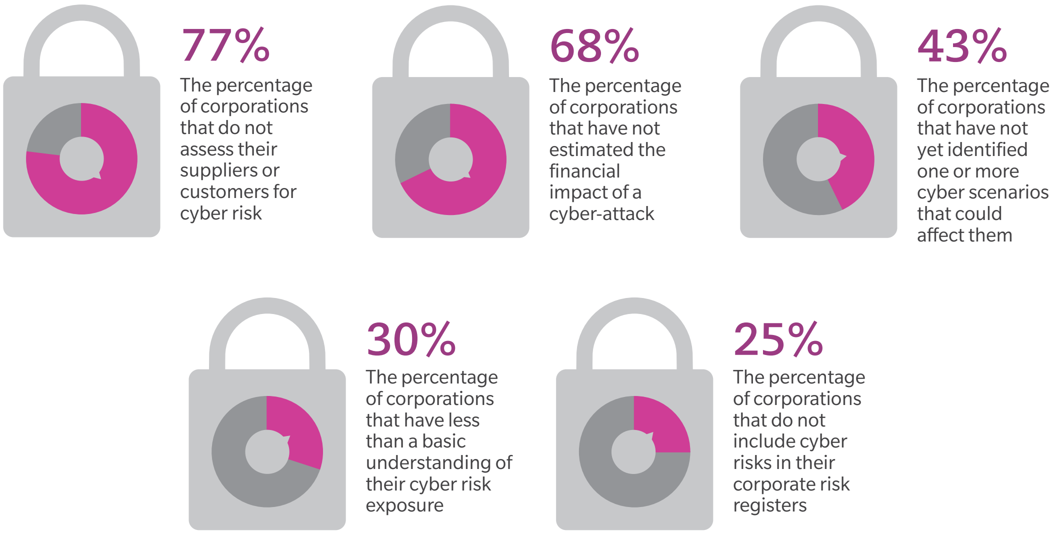
Consider that just last year a half-billion personal records were stolen or lost. Ransomware attacks grew by 35 percent and spear-phishing by 55 percent. These types of attacks are no longer just harming desktop computing. They are starting to cause the malfunctioning of critical medical equipment, emergency services, and fundamental communications. Few organizations' cyber defenses are keeping pace. We estimate that only a third of companies are sufficiently prepared to prevent a worst-case attack. Based on a recent survey by Marsh, Oliver Wyman's sister company, a quarter of companies do not even treat cyber risks as significant corporate risks. Nearly 80 percent do not assess their customers and suppliers for cyber risk.

As companies roll out more digital innovations, they need to adopt more flexible and ubiquitous cyber defense measures to meet the more extreme threats they now face. Failing to do so risks unanticipated costs, operational shutdowns, reputational damage, and legal consequences. For example, in response to growing ransomware and spear-phishing attacks, many leading organizations are drawing up fallback plans to operate offline in the event that their operations are crippled.

Some are going even further and making operating offline their preferred approach: In response to hacktivists crippling the government's websites through a series of cyber-attacks in 2013, Singapore is cutting off access to the internet for nearly all government computers. Healthcare providers and hospitals in the United States and Germany are taking critical systems

THE STATE OF CYBER RISK MANAGEMENT AT A GLANCE

EVEN THOUGH THE NUMBER OF TARGETED CYBER-ATTACKS IS GROWING BY DOUBLE DIGITS ANNUALLY, MANY MEDIUM AND LARGE-SIZED CORPORATIONS STILL DO NOT DEVOTE SUFFICIENT RESOURCES TO CYBER RISK MANAGEMENT



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

68% The percentage of corporations that have not estimated the financial impact of a cyber-attack

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

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

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

Source: European 2015 Cyber Risk Survey Report, Marsh, Global Risks 2015

partially offline where connectedness is not required and are prepared to go back to pen and paper in case an incident impairs their digital operations.

Organizations are also changing the way they use and store data. Classic forms of data and legacy information technology systems are not flexible or smart enough to keep up with rapidly shifting needs to protect records. To respond to cyber threats more rapidly, some companies are radically simplifying their business setups and technical systems. By doing so, companies limit the places where a hacker can enter and hide. Splitting data up and storing the pieces in different systems also reduces the amount of sensitive data vulnerable at any one time.

Other companies are replicating their core information technology systems so clients can receive basic services even if their own systems entirely collapse. For example, some banks are reproducing their key IT systems in the "cloud" to guarantee basic operations can be maintained. Others are striking deals with competitors to step in as proxies in the event of a cyber crisis. These organizations understand that the ramifications of an attack on their systems go far beyond the damage to their own business: An economic crisis could result if millions of businesses and people were suddenly denied access to their accounts, preventing them from being able to pay salaries or bills.

At the same time, leading organizations are examining if adequate safety nets are in place to minimize the aftershocks of cyber-attacks that cascade to the point that they bring down more than one company or industry. Government-backed "cyber pool funds," for example, could mitigate the financial impact of a complete cyber meltdown, similar to funds set aside to assist with the aftermath of terrorist attacks or natural disasters.

The cyber threats that many companies previously considered to be unthinkable are now daily news. To avoid becoming another headline, organizations must prepare for the worst – including the unthinkable.

Claus Herbolzheimer is a Berlin-based partner in Oliver Wyman's Digital practice.