September 2016

K@W

Knowledge@Wharton – NTT DATA

The CFO Imperative: Managing Risks Arising from Technology

Sponsored by NTT DATA

Knowledge@Wharton – NTT DATA

The CFO Imperative: Managing Risks Arising from Technology

As companies become increasingly dependent on technology to perform all aspects of their business — connecting and communicating with customers, suppliers, employees and processing transactions — addressing technological risks becomes a critical part of enterprise risk management. Case studies show that a major cyberattack that leads to stolen customer data can inflict massive damage to a company's reputation and wipe out millions in market value as well. Meanwhile, frequent connectivity problems can lead to market share erosion as unhappy customers leave for your competitors.

Chief financial officers are already familiar with protocols meant to address traditional financial and operational risk factors. But as businesses become more complex and interconnected, CFOs are taking on an expanded role that includes cyber security management. Notes Khirodra Mishra, managing director IT security services at NTT DATA: CFOs face the "downstream impact of security challenges." That means they have to handle the financial and other fallout from data and customer privacy breaches: fraud, eroded customer trust and lost business opportunities, among others.

Proper risk management has a direct impact on the bottom line: A recent EY study shows that the top 20% of companies that deftly manage cyber and other risks perform three times better on EBITDA (earnings before interest, taxes, depreciation and amortization) than firms in the bottom fifth. But for risk management to have maximum effectiveness, it needs to take a holistic approach, says Christopher Ittner, Wharton accounting professor and department chair. "The whole point of enterprise-wide risk management is to break down functional barriers. It's not that companies are not dealing

As businesses become more complex and interconnected, CFOs are taking on an expanded role that includes cyber security management.

with risk. The problem is they are not doing it in an integrated fashion."

The issue is this: Data that could warn about potential risks are usually scattered across different departments in a company. Without the right tools and structure to bring those data points together, companies are hampered in how well they manage risk. Another challenge is that in many companies, there is no consensus on the appetite for risk. "At the very least, you need to have a discussion about the risks," Ittner says. "Risks aren't standalone, so they need to consider their interdependencies and get the cross-functional discussion going." Without adequate risk protection, the inevitable reaction to a breach is immediate crisis management. But usually, such short-term actions distract from planning for longer-term growth.

The bottom line is companies today find themselves in an economy where "uncertainty is high, innovations are disruptive and reinvention is common," according to a paper by Paul Schoemaker, senior fellow at Wharton's Mack Institute for Innovation Management. Traditional tools of risk management are no longer enough. These days, forward-thinking firms need to monitor changes to their ecosystem, conduct a deeper diagnosis of competitive challenges, make bold moves at the right time and redesign business models that co-create and reshape the environment, not just be reactive.

Understanding and Managing Risk

Mishra put technology risks in two clusters. One is the governance, risk management and compliance (GRC) cluster, where technology platforms help develop a structured response such as in auditing, addressing regulatory compliance requirements and others. The other cluster consists of the risks of not using the right technologies, which leads to vulnerabilities.

"The whole point of enterprise-wide risk management is to break down functional barriers. It's not that companies are not dealing with risk. The problem is they are not doing it in an integrated fashion."

— Christopher Ittner, Wharton

Exposure to risks is increased with not just the practice of BYOD — or bring your own device, where employees perform work using their own smartphones, tablets or other mobile devices loaded with their company's applications. It has expanded to include overseeing a practice by some developers, working at client locations, to bring their own storage devices and servers linked to cloud platforms. In a 2015 survey by the Computing Technology Industry Association, nearly half of large and mid-sized companies were concerned about security vulnerabilities introduced through BYOD, closely followed by risks coming in through USB flash drives.

Clearly, an outright ban over the use of such devices won't work. That's why a company's leaders must learn to strike a balance between providing employees and third party developers

the freedom to bring their own devices and technology, and ensuring security of the firm's data. A good rule of thumb in managing cyber security revolves around the concepts behind "CIA – confidentiality, integrity and availability" when it comes to data, applications, systems, processes and the like, says Mishra.

"Confidentiality" refers to company policies that limit access to data or applications only to authorized stakeholders, such as employees and strategic partners. It seeks to protect the data owner's privacy. These policies include the use of data encryption, two-step authentication and storing highly sensitive data in disconnected storage devices, among others.

"Integrity" is about ensuring that the information is accurate, and only authorized stakeholders have the right to modify aspects that impact security. Steps to take include guarding against modifications made by people not authorized to do so or keeping tight watch over different versions of the data to prevent errors being introduced or data accidentally erased. Off-site backups are an option as well in case of accidents such as fires.

"Availability" makes sure users are able to access the data because the network, hardware and software are maintained well. Providing good broadband connectivity so employees can work easily and keeping up with system upgrades are critical.

However, staying true to the CIA security triad can be a challenge due to the volume of data that comes at businesses these days from various sources including social media, the company website, partner sites, internal processes, store locations, mobile devices and the Internet of Things.

Many companies manage risks by involving third party contractors and supply chain vendors by conducting joint analysis of risks, says Ittner. In many rapidly evolving technologies such as cloud computing, individual companies may find they are better off leaving risk management to them. "Cloud

CONFIDENTIALITY – company policies that limit access to data or applications only to authorized stakeholders, such as employees and strategic partners.

INTEGRITY – ensuring that the information is accurate , and only authorized stakeholders have the right to modify aspects that impact security.

AVAILABILITY – users are able to access data because the network, hardware and software are maintained well.

Without adequate risk protection, the inevitable reaction to a breach is immediate crisis management. But usually, such short-term actions distract from planning for longer-term growth.

computing companies like Amazon Web Services and Microsoft's Azure have better cyber security than most companies because they can make large investments in it and amortize it across many clients."

Risk management experts at corporations or their outsourced service providers continuously monitor alerts they receive and run them on "correlation platforms" to identify potential vulnerabilities. Such correlation allows them to potentially predict attacks and respond proactively, Mishra says. "They could inventory the risks and build what are called 'heat maps' that identify minor and major risks, and try to get some cross-functional cooperation so that everybody is on the same page," adds Ittner.

Some providers of risk management services deploy techniques similar to vaccination, which uses pathogens to trigger a body's immune, or defensive, system. These providers have their own trained hackers penetrate a client's firewalls and other security systems to identify points of weakness that then get fixed with software patches and other security tools. Such an approach works because "hackers are often smarter and more innovative [than security experts]," says Mishra. "They are running an R&D lab all the time, trying to hack into your system. At some point, they will be successful."

For companies concerned about the cost, different payment models have surfaced to meet their needs. Mishra says some fraud prevention service providers build the fee into the outcomes. For example, a risk service provider could specify that for every $100 million worth of fraud identified, it collects a fee of $5 million from the client.

"Hackers are often smarter and more innovative than [security experts]. They are running an R&D lab all the time, trying to hack into your system. At some point, they will be successful. … Health care is low hanging fruit for hackers."

— Khirodra Mishra, NTT DATA

A Health Care Case Study

In 2014, hackers targeted three U.S.-based health care companies — Community Health Systems, Premera Blue Cross and Anthem. They stole sensitive information including patient data, Social Security numbers and financial records. Unfortunately, such attacks in the industry are not uncommon. "Health care is low hanging fruit for hackers," Mishra says.

One type of attack targeted against health care companies is holding the data or systems captive until a ransom is paid. Mishra traced the key steps in how a company could respond to such breaches. The first is to ascertain if it is indeed a real attack and not a hoax. The next may be to find out how exactly a payment could be made while checking if paying a ransom violates company policies. But the big question is this: After paying the ransom, how can the company guarantee

the hackers won't strike again? "The hackers are now convinced that the company is amenable to paying to get its data released," Mishra says. At least, in one case he knows, the hackers did not attack the health care company again after it paid the ransom.

But the challenge is to keep up the ongoing fight with hackers without being worn down. That means taking extraordinary measures. "With cyber risks, you can try to mitigate it all you want, but these are rapidly evolving," Ittner points out. "You're never going to stop cyberattacks. Companies have to focus on the mitigation plans and processes they have in place, so that if an attack occurs, they can minimize the damage. They have to stress-test their organizations, and this effort has to come from the board on down."

Risk Management as Growth Driver

There is a flip side to looking at risk management: as a growth driver instead of a loss reducer. Indeed, done correctly, risk management could enhance a firm's enterprise value. A recent study by Ittner shows that firms taking on risk as a value-creation activity as opposed to a loss-mitigation effort were the ones that got the best returns. "There is a risk-return tradeoff. You can't make returns unless you take on risks," he says. "Are you taking on the risk that you want to take on? Risk management is not about minimizing risks. It is about gaining a better understanding of risks and taking on risks that are within your risk appetite, and the type of risk you want to take on because you can manage them better than others."

If your company hasn't experienced a type of risk before, learning from the experiences of others is critical in effective risk management. "One of the issues with risk is you may never have experienced it before but somebody else might have," says Ittner. "By aggregating data from many organizations, you could model and identify risks and fix them."

"You're never going to stop cyberattacks. Companies have to focus on mitigation plans and processes they have in place, so that if an attack occurs, they can minimize the damage."

— Christopher Ittner, Wharton

Mishra adds that the challenge for organizations today is to create an environment where technological innovation is encouraged while making the ecosystem more secure and resilient. He likened a CFO's role with that of a brake in a car. "The role of a brake in a car is not just to slow it down but to give the driver the confidence and comfort to drive fast," he says. "CFOs should put in place the right controls and mechanisms so that business can grow faster, without the fear of failure from a technology and process standpoint."

In summary, as today's corporations embrace new technologies and are deluged with Big Data, they also expose themselves to risks that expand at a similar rate. Left unmanaged or caught unprepared, these risks threaten their business fortunes and reputations. However, corporations that take calculated risks and see risk management as a value-creating activity could well see higher growth and an increase in enterprise value.

A Risk Management To-do List

- ✔ Create a holistic risk management platform. Many organizations conduct risk management within silos.
- ✔ Seek ways where the risk management effort helps bring competitive advantage as well to drive superior performance across the organization.
- ✔ Identify employees or employee groups using personal devices that could pose a security risk.
- ✔ Find clusters of data, applications and other systems that each employee or employee group is permitted to access, and build fortifications around those.
- ✔ Develop your own threat-management platform or subscribe to a third-party platform and run your analytics there.
- ✔ Look for weak links in the company's intranet and develop a risk mitigation plan around it.

This article was produced by Knowledge@Wharton, the online business analysis journal of the Wharton School of the University of Pennsylvania. The project was sponsored by NTT DATA.

Founded in 1881 as the first collegiate business school, the Wharton School of the University of Pennsylvania is recognized globally for intellectual leadership and ongoing innovation across every major discipline of business education. With a broad global community and one of the most published business school faculties, Wharton creates economic and social value around the world. The School has 5,000 undergraduate, MBA, executive MBA, and doctoral students; more than 9,000 annual participants in executive education programs; and a powerful alumni network of 94,000 graduates.

About Knowledge@Wharton

Knowledge@Wharton is the online business analysis journal of the Wharton School of the University of Pennsylvania. The site, which is free, captures relevant knowledge generated at Wharton and beyond by offering articles and videos based on research, conferences, speakers, books and interviews with faculty and other experts on current business topics. Knowledge@Wharton offers content in Chinese, Spanish and Portuguese and has a separate site for high school educators and students.

For more information, please visit knowledge.wharton.upenn.edu

About NTT DATA

NTT DATA partners with clients to navigate and simplify the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. We deliver tangible business results by combining deep industry expertise with applied innovations in digital, cloud and automation across a comprehensive portfolio of consulting, applications, infrastructure and business process services.

NTT DATA is a top 10 global business and IT services provider with 100,000+ professionals in more than 50 countries, and is part of NTT Group, a partner to 85% of the Fortune 100.

To learn more about NTT DATA, please visit: http://www.nttdataservices.com/en-us/Services