AlixPartners
when it really matters

FINANCIAL SERVICES

FEBRUARY 2017

Cybersecurity: watch your bytes

You hear on social media or the radio that the bank where you are an executive has been hacked. You knew nothing about this and you are already behind the news cycle.

Your customers' life savings have been depleted overnight. Your systems remain frozen no matter what your IT team does and can't perform even its day-to-day functions. Personal and systemic data are being stolen or deleted. Money is being stolen or created anew at the whims of cyberbarbarians. Both retail and corporate clients are panicking, and domestic and international markets are experiencing severe dislocations, followed by paralysis of the global financial system's main fundamental functions.

The reputation and value of your business will likely reduce immediately. Churn will increase, and before regulators have even begun to assess you, your losses will impact your EBITDA. If the breach is significant, shareholders and stakeholders will hold you responsible and probably accountable. After a breach is not the moment to determine your cyberrisks and vulnerabilities, and it is too late to prepare for the press conference (where you will be expected to speak) with any degree of confidence or substance. It will not matter whether or not you are the Chief Information Security Officer (CISO), because security is at the heart of any financial business and should be on everyone's agenda.

As the Internet of Things rapidly approaches, we could potentially lose control of devices that society counts on every day, like home appliances and self-driving cars, not to mention nuclear reactors and warfare systems that are digitally controlled.

Faced with those growing threats, banks can no longer afford to take a tick-the-box approach to cybersecurity. They must design comprehensive programs that use the best technology available for measuring and analyzing cyberrisk. What's more, they have to hire and empower dynamic CISOs to run those programs and lead them down an entirely different path toward solid and reliable cybersecurity programs.

Cybersecurity losses are mounting

- Average cost incurred for each lost or stolen record containing sensitive and confidential information: $158[1]
- Average time to detect malicious attacks: 229 days[1]
- Losses resulting from malicious activity: 48%[1]
- Identities exposed in 2015 (23% yearly increase): 429 million[2]
  - At Tesco Bank, 40,000 accounts were hacked. Around 9,000 customers had money stolen, and the bank had to repay £2.5 million to customers.[3]
  - At Bangladesh Bank—Bangladesh's central bank—$81 million was stolen by way of rogue Swift software transfers.[4] Up to 12 banks were affected by the same attack.[5]
- Target's cyberbreach cost the company £162 million.[6]
- Yahoo reported in 2016 that more than 1 billion records had been stolen in 2013.[7] Now Verizon appears to be re-evaluating the deal to buy the technology company.

BARBARIANS AT THE PORTAL

A number of cyberbarbarians are likely waiting at the global financial system's portal, ready to exploit any weakness. The result of a weakness could be collateral damage the nature of which is hard to predict and potentially too widespread to contemplate. Guided by the relentless pace of technological innovation, data quantities are growing exponentially, the Web is becoming more and more ubiquitous, and digital systems are becoming more and more embedded into everyday life.

Groups of cyberterrorists and hacktivists and groups of cyberrobbers and spies tend to have different motivations. The former seem to want to wreak havoc on vital economic and social systems, and the latter seem to want to steal money, critical financial intelligence data, and trade secrets. But their methods look increasingly similar, as do their targets, with the global financial system and its main intermediaries being among the most popular.

Let's consider European banks, for example.

Appearing to be sitting on an unstable ("not really investable as a sector," in the words of Credit Suisse CEO Tidjane Thiam[8]) business model, many European banks are now trying to digitally transform themselves—for example, by playing digital and thinking digital.

Banks' traditional business model has been based on three pillars of so-called unbearable lightness.

- Banks multiplied the money supply by leveraging their equity capital, getting funds from multiple low-risk sources, and giving the funds away to fewer, riskier lenders so they could build an interest rate spread for themselves.
- Banks multiplied that fungibility across time and space, building time and geographic mismatches into their balance sheets to further enhance that spread on normally upward-sloping term structure yield curves.
- Banks multiplied their share of principal investing and risk underwriting, thereby increasing the density and velocity in their equity capital usage by way of structured derivatives and asset securitization.

Banks are now trying to reinvent themselves as "digital" on the basis of the following few building blocks.

- Data and information accumulation, preservation, extraction, and management.
- Applied analytics and artificial intelligence to derive intelligence.
- The development of new ways of interacting with customers via omnichannel distribution that lets them sit still in the middle of the intermediation/interconnection game.
- The identification of new business solutions and customer novel-use cases that provide real value.
- Operating on the basis of trust and credibility as the starting points and founding blocks of the industry.

[1] 2016 Ponemon Institute Cost of Data Breach Study.
[2] Symantec Internet Security Threat Report 2016.
[3] Martin Arnold, "Tesco Bank 'ignored warnings' about cyber weakness," Financial Times, November 13, 2016.
[4] Michael Corkery, "Hackers' $81 Million Sneak Attack on World Banking," New York Times, April 30, 2016.
[5] Michael Riley and Alan Katz, "Swift Hack Probe Expands to up to a Dozen Banks beyond Bangladesh," Bloomberg, May 26, 2016.
[6] Target 2014 Q4 earnings report.
[7] Vindu Goel and Nicole Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked," New York Times, December 14, 2016.
[8] Laura Noonan, "Europe's banks 'not really investable' says Credit Suisse's Thiam," Financial Times, September 28, 2016.

A BIT OF CREDIBILITY

More than ever before, credibility is everything. It takes a lot for banks to build credibility in the digital space—and just a little bit to lose that trust.

Under banks' new digital strategies, the intangibility of the unbearably light, "not really investable" business model is even greater and is based on the quantity and quality of the data and information being managed. If a cyberattack harms those attributes, the very basis of the operating model is put at risk. Further, if the intelligence that banks' systems produce gets sabotaged, lost, or stolen or if their systems freeze and disrupt their day-to-day functioning, then their entire added value to the economy can be undermined. For banks, everything is built on trust or, actually, cybertrust. Cybertrust is becoming an extremely important and scarce resource that stakeholders must preserve. It is best allocated across multiple risk and return opportunities and must be managed accordingly like other limited resources whether they are tangible or intangible in nature.

That credibility, built through the course of many years and based on the careful management of trillions of bits and bytes, can be measured. A bank's cybertrust or cybercapital can and should drive its digital business and operational strategy. Unfortunately, cybersecurity has turned into a buzzword usually associated with a tick-the-box mentality that relies too heavily on vendor software solutions. Banks must begin taking a more holistic approach.

Important cyberrisk questions to answer

- What are your company's critical business processes and assets?
- What would the financial, reputational, and compliance business impact be in the event of a loss of data availability, data confidentiality, and data integrity?
- What cyberthreats are common in your industry?
- What is the likelihood of cyberthreat?
- What countermeasures with regard to processes, people, and technology are in place to mitigate cyberrisks?

CYBERINSECURITY

Businesses have to get the basics right and avoid simple blunders. They can start by concentrating on the physical safety of their data and their environments. People management of employees, customers, and suppliers alike is of course a good starting point as well as a must-have. But the road to a more scientific yet still pragmatic way of managing cyberrisk must include some form of objective quantification. The management of cyberrisk is not an actual end in itself but a necessary means to a business goal.

Let's start by clarifying that the term cyberrisk quantification refers to the process of evaluating, measuring, and analyzing the cyberrisk that the bank or any other financial intermediary has identified. The analysis should take advantage of all available cyberdata and information by using the most-sophisticated modeling techniques—from traditional conjoint statistical analysis to black-box techniques such as neural networks, fuzzy logic, genetic algorithms, and various artificial intelligence applications.

The analysis could then work out how to accurately and dynamically represent the organization's cyberenvironment—for instance, by using a Monte Carlo simulation to run millions of cyberattack outcomes to derive the organization's estimated loss distribution. The analysis should cover all business-critical applications, databases, IT systems, and associated exposures in dollars by reflecting both direct and indirect potential losses such as:

- Costs of straight-through robberies regardless of their full or partial cover from the bank's side.
- Costs arising from potential disputes with customers and even suppliers and employees in case their personal, confidential data gets stolen and used fraudulently.
- Regulatory fines associated with compliance failures, as well as the regulatory-capital-requirements top-up associated with a weaker cybersecurity system—via the operational risk capital requirement.
- Disruption in day-to-day operations, with potential business losses and reputational harm.
- Broader and more-persistent damage to the bank's brand that would impair its commercial goodwill or its ability to attract the best digital talent in the market.

On the basis of those potential losses and their expected frequency, their expected impact should be calculated in two separate but complementary ways:

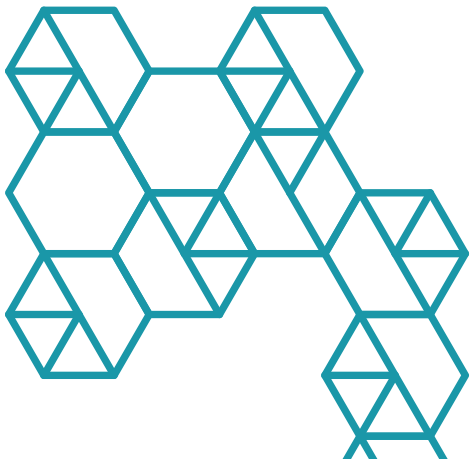
1. As the maximum unexpected loss value for a given level of confidence that drives capital buffer need.
2. As the mean of the same distribution that should be considered and then built into the pricing structure of any product or service on the basis of the product or service's cyberriskiness and given the target return on cybercapital.

That as-is analysis of digital business and operating model riskiness should then be matched by considerations about the bank's network topology, the defenses that have been put in place based on specific cyberframeworks, the strength and maturity of each framework, and so on. That means that cyberattacks' success rates and collateral damages are not built into a vacuum. The CISO should not aim only at identifying, evaluating, controlling, and monitoring existing or emerging cyberthreats but also at proactively and reactively managing them.

- Many cyberattacks may potentially be prevented and their success rates reduced significantly if scarce resources are critically aligned and focused on the unacceptable risks. Businesses should allocate portions of their budgets to projects that can maximize the return on cybercapital.
- Cyberattacks are, however, never fully avoidable, and so, the reactionary part of the CISO's job is as important as the proactive one. The CISO should drive loss minimization by addressing all direct and indirect damage associated with robbers, terrorists, spies, and others.

Business as usual: an example of how banks typically approach cybersecurity

- Identify and govern cyberrisks:
  - Banks focus mainly on compliance (e.g., European Central Bank, Payment Card Industry Data Security Standard, privacy, General Data Protection Regulation).
  - But banks tend to:
    - Lack security governance, including strategies and plans for improvement, for training and awareness, and for roles and responsibilities.
    - Lack IT risk management from a business perspective.
    - Lack asset management, including data governance, and particularly classification and prioritization.
- Protect against cyberrisks:
  - Banks are usually well-covered. So far, they've typically allotted the main portion of their security budgets to security hardware and software.
- Detect cyberrisks:
  - But banks also usually lack security incident management or security incident detection inside their IT incident processes and procedures.
  - Banks' roles and responsibilities are usually not clear, particularly in outsourcing environments.
- React and recover from cyberattacks:
  - Banks make investments mainly in data availability for business continuity.
  - Banks take a typical technical-response-and-recover approach and focus less on people and processes.
  - Banks likely have no processes-and-procedures tests.



THE CISO

There is a clear link between credibility and trust and between cybersecurity and the better management of cybercapital. The CISO should:

- Design the best risk management system that includes organization, processes, models, and IT infrastructures and applications aimed at addressing cybersecurity as the key risk. The CISO should coordinate closely with the chief risk manager on bankwide risk aggregation projects.
- Design a planning and control system that includes targeting, budgeting, and reporting on risk-adjusted performance. Such a system should be one that helps the chief financial officer make best use of the bank's capital. It should also help the chief operating officer correctly define optimal cost structures. And it should help the chief information officer or chief technology officer design the best cyberrisk-consistent IT system.

Drawing on the comprehensive analysis and objective quantification of the cybercapital at risk, the CISO should determine the best proactive and reactive courses of action—including strategies that would hedge or cover part of the cyberrisk via insurance guarantees, for example—and execute them.

As a warden of cybertrust and a guardian of the cybercapital at risk, the CISO should frequently report to the CEO and the chairperson. Together they should regularly discuss the ever-evolving cyberrisk taxonomy the bank faces and how the bank plans to deal with it based on the risk/return appetite of its stakeholders.

Far from being a mere tick-the-box solution, this approach promises to lead to very interesting and challenging discussions with the executive team.

THE CYBERSPACE TO COME

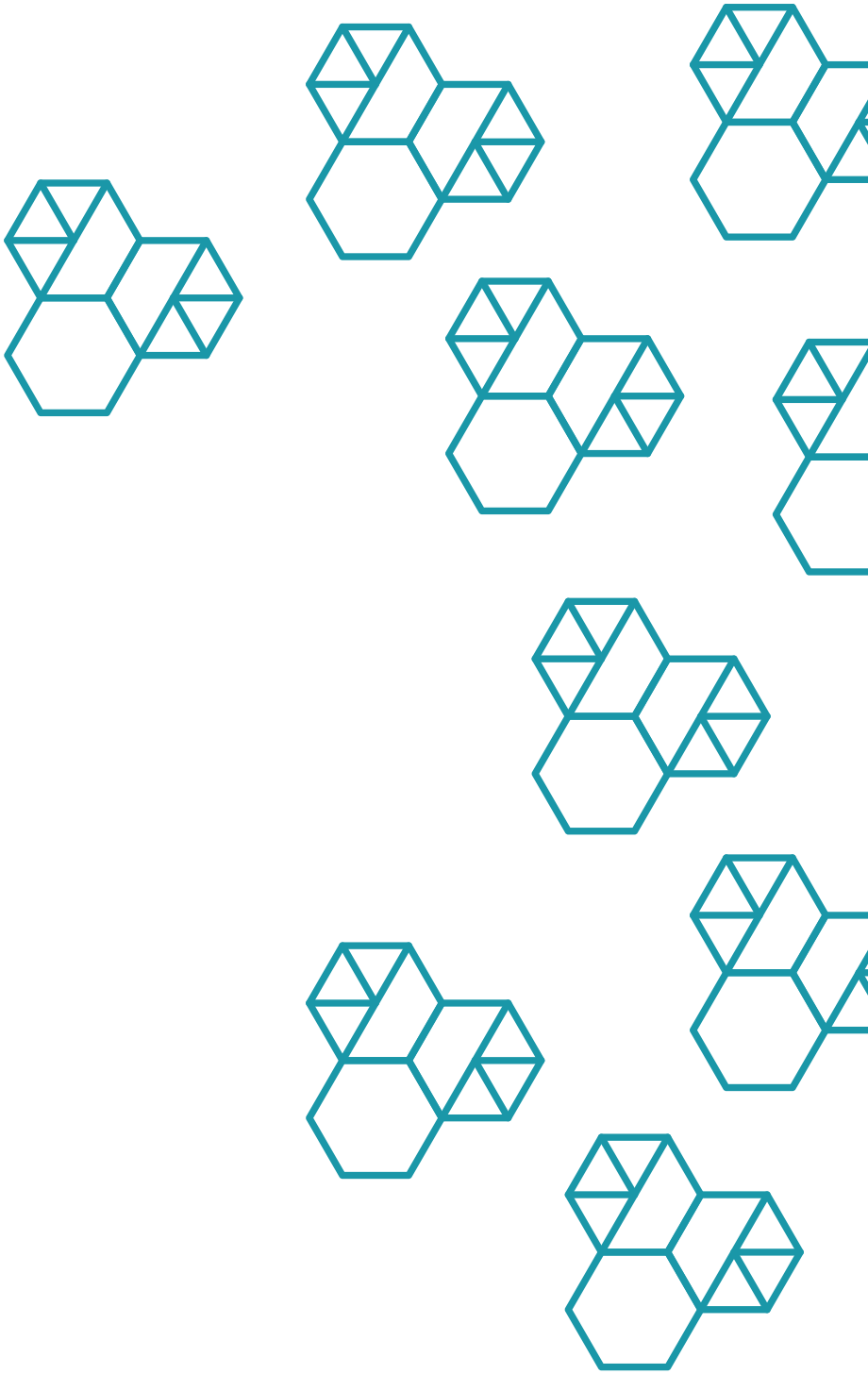
Cyberspace, a term coined by science fiction writer William Gibson in 1982, has come to represent what Gibson described as the "consensual hallucination experienced daily by billions of legitimate operators."[9] The threat of attacks against that "hallucination," which includes the global financial system, is looming larger every day. Former US President Barack Obama in 2014 called cyberattacks "one of the gravest national security dangers" his country faces.[10] In fact, cyberthreats pose a grave danger to not just one society but also the very fabric of the global economic system and the civil societies it underpins.

Although banks and financial institutions have to accept that a zero-risk policy is unattainable, they must work to keep unacceptable risks at bay. Long past is the time of cyberrisk checklists and quick fixes or vendor solutions for everything. It should be a routine topic of discussion for boards and committees that constitutes good and normal governance of a business. Delivery and assurance can be delegated, but responsibility for the impact of a breach on the balance sheet and value cannot. Banks have to invest in strong CISOs who will help take a fundamentally different approach to cybersecurity by way of both proactive and reactive risk management. A CISO must have the right to call the shots—from the organizational and resources perspectives. Far from being the geek that nobody wants to work with or a former hacker making amends, a CISO must be a talented leader with a gift for digital. **A**

The CISO's new role and approach

- Manage cybersecurity risks in connection with the enterprise risk management team to discover business opportunities.
- Evaluate and implement cybersecurity countermeasures, prioritizing them against related business risks.
- Engage with the board on the issue of company cyberawareness and to justify cybersecurity investments for business risk mitigation.
- Take an active role in the analysis and design phases of new business opportunities at very early stages.

[9] www.web.mit.edu/m-i-t/provocations/gibson.html.
[10] www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.



CONTACT THE AUTHORS:

Lorenzo Grillo and Claudio Scardovi.

FOR MORE INFORMATION, CONTACT:

Claudio Scardovi
Managing Director
+44 20 7098 7615
cscardovi@alixpartners.com

ABOUT US

In today's fast paced global market timing is everything. You want to protect, grow or transform your business. To meet these challenges we offer clients small teams of highly qualified experts with profound sector and operational insight. Our clients include corporate boards and management, law firms, investment banks, investors and others who appreciate the candor, dedication, and transformative expertise of our teams. We will ensure insight drives action at that exact moment that is critical for success. When it really matters. alixpartners.com