LEADING EDGE FORUM

Executive Summary

A Board Guide to Cyber Risk

Michael Bufalino
Dave Aron

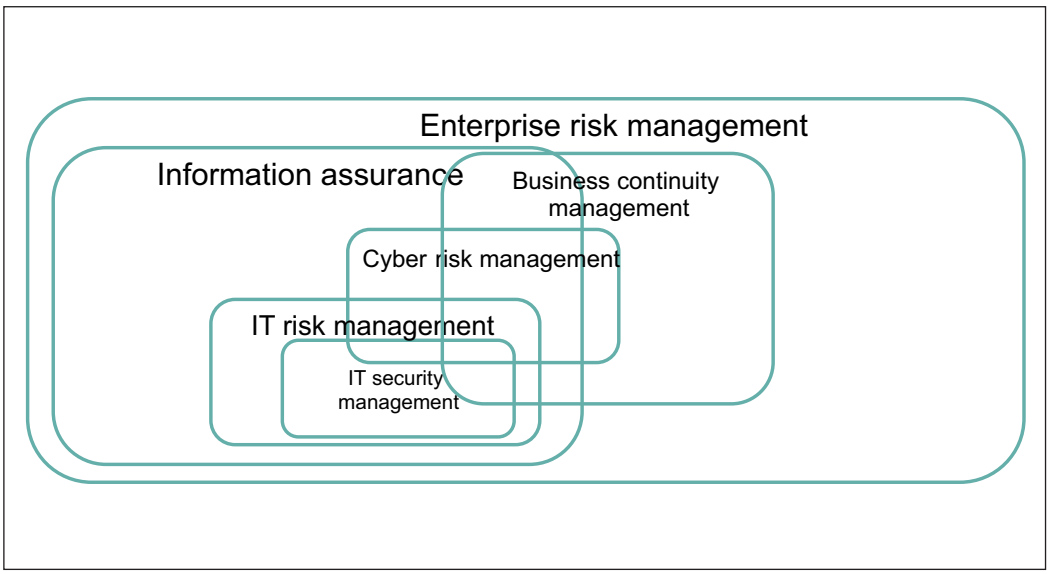
August 2017

There is an ongoing cyber-security arms race between every organization and the bad guys; but we believe that over and above that, it is imperative for the most senior leadership of each organization to find clarity, build a mental model and implement decision-making mechanisms to address this mega-issue. In this report, we specifically address the question: *How can we get boards of public- and private-sector organizations to make better decisions around cyber risk?*

LEF uses the following working definition:

> *Cyber risk management is the discipline that focuses on managing the risks to a company, country or other entity arising from intentional attacks through electronic means.*

Cyber risk is a part of the risk management family, as shown in Figure 1. (Note that there is no single, globally agreed view, but risk experts probably wouldn't be shocked or in violent disagreement with anything here.)



Cyber risk management is part of overall enterprise risk management

Cyber attacks come in many forms, including hacking, ransomware, denial of service attacks, phishing, malware, viruses, insider threats and advanced persistent threats.

At the time of writing, we are emerging from the aftermath of the WannaCry[1] ransomware incident, which had implications way beyond the financial. (It is extra-interesting because it seems that the WannaCry code may have been acquired from the US National Security Agency.) It seems pretty clear to all of us that we are in a very precarious place when it comes to both the likelihood and the impact of cyber incidents. Meanwhile the shadow of the rapidly approaching EU General Data Protection Regulation (GDPR) and its equivalents looms large.

1. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Our precarious position with regard to cyber risk

We are in a pretty dark place, in regard to cyber risk, and the challenges are getting worse

Ever since computers were a thing, there has been a dark side to the digital story in terms of security and privacy. More recently, as information technology is increasingly not only mission-critical (we can't run without it) but also strategic (a major differentiator/source of competitive advantage), the stakes have risen considerably.

Cyber-attack surfaces[2] have increased as digital business pervades – for example, they now include the cloud and the internet of things – and whole new, unexpected attack vectors are possible. The cost and risk implications are often substantial, sometimes existential. Cyber-insurance is relatively immature, poorly understood and not very well penetrated into the market.

DXC.technology

"Information risk is the truly existential cyber risk for most organizations."

Dan Hushon, SVP and CTO, DXC

To compound the issue, those seeking to cause cyber damage are growing in number, diversity and sophistication, because the motivations are increasing. For example, Symantec claims that 1 in every 131 emails in 2016 contained a cyber threat[3]. The bad actors range from naughty geeks causing mischief, through organized cyber-criminals and hacktivists (those hacking for a cause), all the way to state-sponsored cyber attacks. The financial cost of initiating a cyber attack is low, and there is often little recourse, and unclear or weak jurisdiction – which all encourage cybercrime and do little to deter would-be cyber-hackers. What's more, the cyber war is asymmetric (like terrorism): the good guys have to win every time, but the bad guys can try many times, in many ways, and only need to succeed once.

The profile, pervasiveness and scale of cyber incidents is eye-watering. The table below shows a number of recent examples.

2. The 'attack surface' is where cyber attacks happen – all the different points where an attacker could get into an IT system or get data out.
3. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Incident	Details
SWIFT	Bangladeshi bank hack: criminals attempted to divert $951 million using Swift, but only succeeded in transferring $81 million.
Dyn	Record-level denial-of-service (DoS) achieved using the IoT as a network of zombies (infected with the Mirai botnet). The motivation was apparently hacktivism in response to Julian Assange's internet access being revoked. High-profile organizations impacted included Airbnb, Amazon.com, BBC, CNN, DirecTV, Fox News, HBO, NHL, Netflix, *The NY Times*, PayPal, Pinterest, Spotify, Twitter, Visa and Walgreens.
YAHOO!	500 million - 1 billion user accounts disclosed. This ultimately resulted in a negative re-valuation (of the order of $350 million) in the subsequent Verizon acquisition.
D	Democratic National Committee (DNC) email hack: a political attack to embarrass and discredit the Democratic party during the US presidential election. The trend of political interference continues, the latest being the French presidential election in May 2017.
MADE IN Stuxnet U.S.A.	The US (and Israel) used the Stuxnet worm to slow down the Iranian nuclear programme. Stuxnet is a polymorphic worm, difficult to stop as it is always changing.
BLACK ENERGY	BlackEnergy malware took parts of Ukraine's power grid offline. Around 250,000 people were without power for hours and some substations were not fully functional for months after the incident.
ORACLE	A point-of-sale system attack gained access to approximately 700 cash machines.
Dropbox	68 million user accounts were breached in 2012. (This was revealed in 2016.)
ASHLEY MADISON.COM	Hacktivism against people conducting extramarital affairs. In excess of 70Gb of personal data is believed to have been breached.
	WannaCry ransomware (cryptoworm) attack. In May 2017, 230,000 computers in 150 countries were hit within 1 day and ransoms demanded.

Some recent high-profile cyber incidents

A cyber-savvy board is now table stakes

Despite all the incidents mentioned above, the evidence suggests that cyber risk remains a major challenge for boards, by their own estimation. This is partly because cyber risk remains an amorphous, somewhat-abstract domain that boards struggle to get their heads around. What are the boundaries? Is it an IT issue? How does it relate to other forms of risk? Most people, including most board members, don't have a mental model that cyber risk neatly maps into. Also, they find the idea that the journey is never over – in that new risks are continually popping up and one can never be 100 percent safe – confusing and dispiriting.

Given that cyber risk represents an existential threat to every organization, and has huge legal, regulatory, brand and other implications, we have to start at the top: the board of directors, or whatever the most senior oversight group is called. A simple, but crucial, place to start is ensuring that the board membership includes people with appropriate experience and knowledge. Our research suggests that while it is of course helpful to have deep cyber risk knowledge on the board, what's even more significant is sufficient participation by people with deep knowledge of the IT/digital domain in general.

Several of the companies and experts that we spoke to during the course of this study, as well as the personal experience of the two authors, confirm that this digital skills gap at the board level is very real, in terms of both executive and non-executive directors (NEDs). The question of why that is the case is a tricky one to answer, but may involve those who are traditionally in power having a skewed, out-of-date view of cyber risk as a lower-level functional consideration, and those at board level being reluctant to make way for others with different and newer skill sets.

CSO confidential

"Board understanding of cyber risk tends to be patchy and goes through a maturity curve. It is crucial for boards to reflect honestly as to whether they have sufficient cybersecurity capability."

Paul Dorey, Director, CSO Confidential

Four levers to pull to achieve a cyber risk mindshift

In this report we outline four approaches that help achieve a positive shift in the cyber risk management mindset of the board:

1. Achieve a shared understanding of your board's current cyber risk management capability

The full report contains a checklist that we recommend clients use to assess the board's current cyber risk capability at a high level. As with all high-level checklists, the goal is not to obsess about the exact scores for each section, but to generate awareness and discussion, and to highlight blind spots and over-confidence. One of the best ways to do this is to get each member of the board to score the board as a whole, then compare and contrast the results. Techniques to increase the cyber-savvy of the board – or at least the urgency to do so – include running simulations of incidents, commissioning formal audits, and getting experts in to speak to the board.

2. Leverage the principles of antifragility

We at LEF are enthusiastic about the concept of antifragility and believe it holds lots of value potential. In *Rethink Risk Through The Lens of Antifragility*, we identify nine behaviours that create conditions of antifragility. In terms of cyber risk management, the antifragile practices of bringing the dark side inside, tinkering aggressively, creating modular, distributed, redundant operating models, diverse workforce and amplifying sensing and learning capabilities can all contribute very strongly.

3. Lean into frameworks

Although we warn against an over-reliance on detailed standards earlier in this report, we do recommend using an existing high-level framework, such as the NIST Cybersecurity Framework (https://www.nist.gov/cyberframework) to guide your cyber-security/risk activities. There is no point reinventing the wheel, and many of these standards are very well thought through.

4. Apply an ecosystem perspective

Modern business is characterized by connected ecosystems. Gone are the simple days when a company, disconnected from all others, bought raw materials, processed them, then sold them to customers. Almost everyone is connected to the internet, for good and bad. Some companies participate in digital marketplaces, such as the airlines' GDSs (Global Distribution Systems – Amadeus, Sabre, Galileo, Worldspan). Some are linked in industry consortia. This connectedness represents both threat and opportunity for cyber risk management – for example, rapidly sharing threat information with trusted partners. In short, when it comes to cyber risk management, it takes a village.

In summary, cyber risk is evolving faster than the board's ability to cope with it. We are in a terribly precarious position, and the stakes are very high. The solution does not lie solely in technical or front-line behavioural evolution; there must be change at board level. We can't guarantee a cyber attack will never succeed, but by improving the board's understanding of cyber risk using the approaches described in this report, we can cushion the blow by reducing its likelihood, impact and time to recover.

LEADING EDGE FORUM

Regional Headquarters

The Americas
1775 Tysons Blvd
Tysons, VA 22102
USA

3000 Hanover St
Palo Alto, CA 94304-1112
USA

Asia, Middle East, Africa
Level 9, UE Biz Hub East
6 Changi Business Park Avenue 1
Singapore 468017
The Republic of Singapore

Australia & New Zealand
26 Talavera Road
Macquarie Park, NSW 2113
Australia

North and Central Europe
Schickardstrasse 32
71034 Boeblingen
Germany

South Europe
Tour Carpe Diem
31 place des Corolles
CS 40075
92098 Paris La Défense Cedex
France

UK and Ireland
Floor 4
One Pancras Square
London
N1C 4AG
United Kingdom

United Kingdom
Bracknell/Amen Corner B1-2, UK
Cain Rd. Amen Corner (Blgd BRA02)
Bracknell RG12 1HN
United Kingdom

About DXC Technology

DXC Technology (NYSE: DXC) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private- and public-sector clients across 70 countries. The company's technology independence, global talent and extensive partner alliance combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.

Evolution 75 Silk is an FSC certified recycled paper and board range manufactured using 75% post consumer recycled fibre and 25% virgin fibre of which 70% is FSC certified. Evolution 75 Silk carries the FSC Mix label.

evolution™

Leading Edge Forum

Asia Pacific and Australia
135 King Street
Level 20, Sydney
NSW 2000
Australia

France
Tour Carpe Diem
31 place des Corolles
CS 40075
92098 Paris La Défense Cedex
France

Germany, Austria and Switzerland
Römerstrasse 11
D-82049 Pullach
Germany

United Kingdom, Ireland, Iberia, Italy, Benelux, The Nordic Region and South Africa
Floor 4
One Pancras Square
London
N1C 4AG
United Kingdom

United States and Canada
1775 Tysons Blvd
Tysons, VA 22102
USA

About Leading Edge Forum

Leading Edge Forum (LEF) is a global research and thought leadership programme dedicated to helping clients reimagine their organizations and leadership for a tech-driven future. We serve as a strategic touchpoint for CXO teams to provoke and challenge their thinking to help them win in the 21st century.

We believe that as business and IT become inseparable, virtually every aspect of work and the modern firm will need to be reimagined, and this creates exciting new digital opportunities.

Through an annual membership programme of research, events, onsite workshops and advisory services, we support senior leaders in areas such as strategy, organizational change, executive education, talent development and the future of the IT function. Members enjoy personalized access to our global network of thought leaders, clients and leading practitioners.

Leading Edge Forum is part of DXC Technology. For more information, visit leadingedgeforum.com.