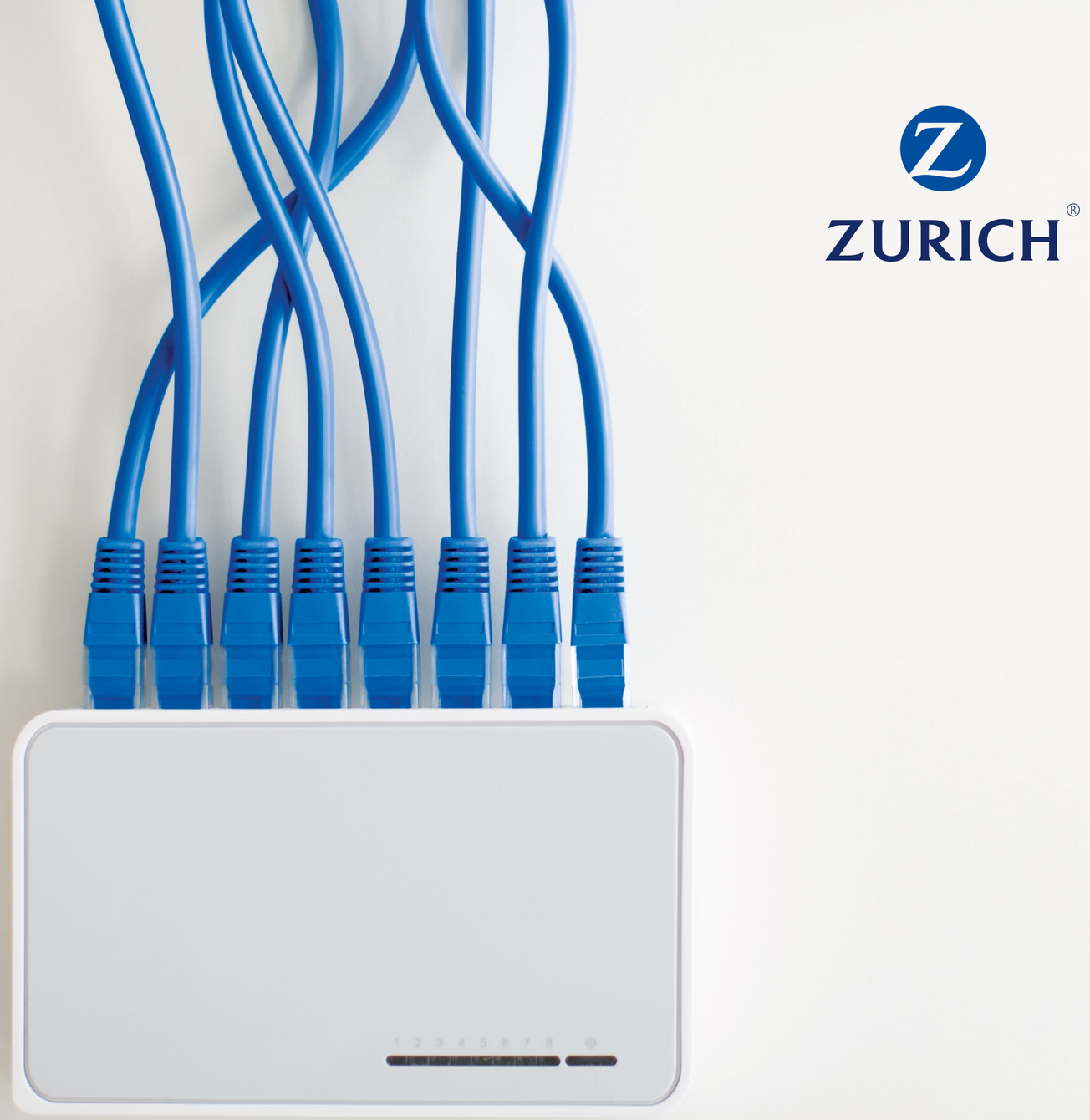
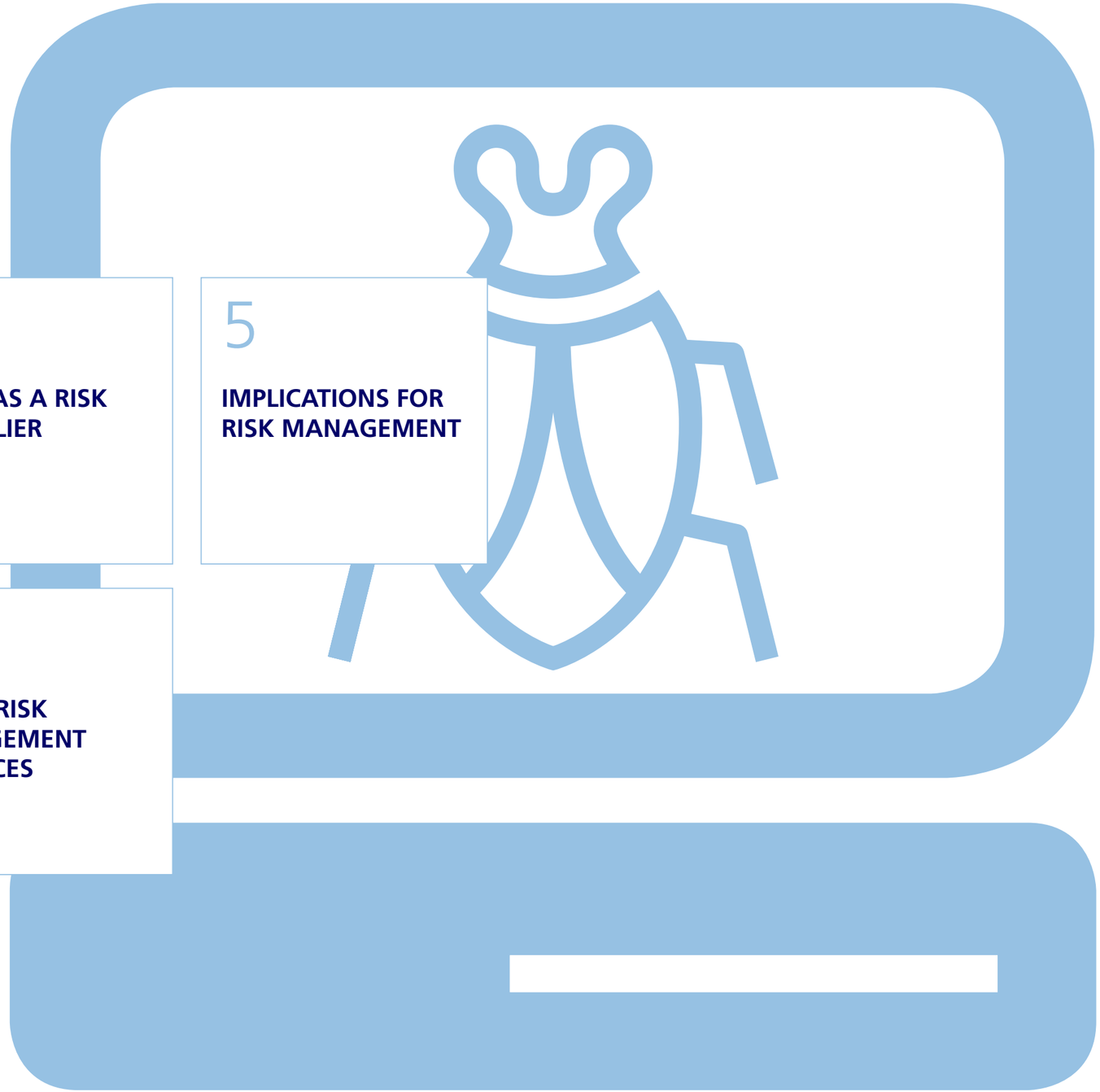
Global Risks Insights
Cyber Risks

Cyber risks scenario for business

Counting the cost of growing societal threats



CONTENTS



Counting the cost of growing societal threats

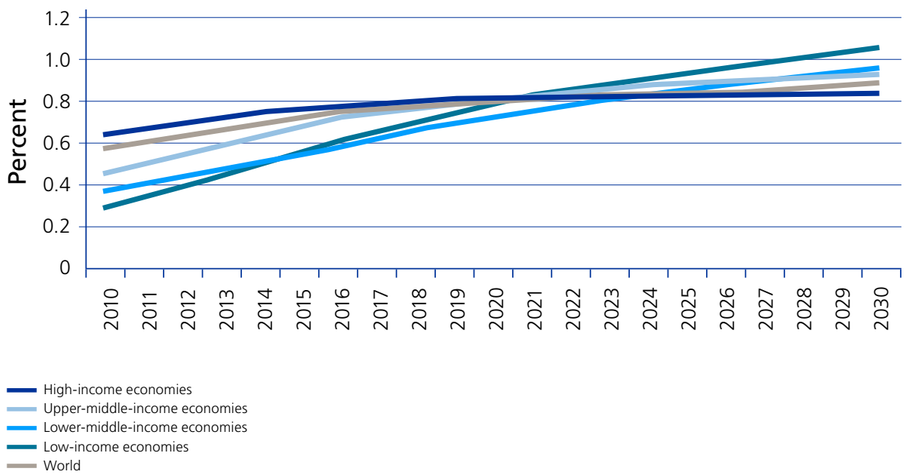
By 2030 cybersecurity costs are likely to double and the cost of adverse events could reach USD 1.2 trillion, or 0.9 percent of global GDP[1].

While those costs would still rank well below those of international violence[2], the threat to critical infrastructures – such as energy – is growing.

Another danger is that trust in cyber-based technologies could be so undermined that implementation of new cost-saving technologies – such as networked healthcare – could be slowed.

Recent ransomware attacks such as WannaCry and Petya, which have affected millions of computers on over 150 countries, have served to heighten the awareness of network vulnerabilities and business continuity responses. There is no doubt that frequency and severity of such attacks will only increase in the future.

ICT cyber adverse events costs, annual total, by World Bank country income group, Percent of GDP, 2010-2030



Source: International Forecast Model of Pardee Centre at University of Denver 7.15

Cyber Attacks Against Critical Infrastructure

The World Energy Council has warned that cyberattacks against energy infrastructure are growing more "sophisticated" and "frequent"[3] and that businesses and politicians are underestimating the risks[4].

The economic and social costs of a "blackout" would be huge. A Lloyds study thought they could reach as much as $1 trillion if attacks on several electricity generators in the US resulted in a grid failure[5].

In late 2015 a power grid in western Ukraine was brought down for six hours, resulting in widespread electrical outages in Western Ukraine and leaving 103 cities without any power and a larger number partially blacked out. Because call centers were also disabled, customers could not report their outages. On-site interventions had to be maintained for weeks afterward.

The World Energy Council has identified ten other serious "incidents" of cyberattacks on power grids and other energy-related infrastructure, mostly in the last several years[6].

[1] Ibid.
[2] Institute for Economics and Peace, "2015 Global Peace Index Report," June 2015, http://economicsandpeace.org/wp-content/uploads/2015/06/Global-Peace-Index-Report-2015_0.pdf.
[3] Ibid., p.
[4] Jessica Morris, "World Energy Council: Cyber threat to world energy," City A.M., April 17, 2016, http://www.cityam.com/239053/world-energy-council-cyber-threat-to-world-energy.
[5] Gabrielle Desarnaud, "Cyber Attacks: A New Threat to the Energy Industry," IFRI, July 7, 2016, p. 3, https://www.ifri.org/sites/default/files/atoms/files/edito-desarnaud_cyber_attacks_energy_industry_eng2.pdf.
[6] "World Energy Perspectives 2016," World Energy Council, pp 4-5, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/World%20Energy%20Perspective%20Executive%20Summary-09-2016.pdf.

Cyber as a Risk Multiplier

Cyber Attacks Against Energy Infrastructure

The Shamoon virus which "infected 30,000 computers belonging to Saudi Aramco,"[7] forced business systems offline for 10 days in 2012. Eighty-five percent of the Saudi Aramco's hardware was decimated. But it could have been worse. Oil production was able to continue because Aramco heavily invested in cyber security of its operations. Business transactions, however, had to be handled on paper and it took Aramco five months to recover.

Historically, systems running operations were often very tailored and proprietary so not as susceptible, but recently more off-the-shelf software has been adopted for business and industrial entities which has heighted the threat[8]. Attackers also use backdoors entries from the business or other entities to attack key operations. Remote control of some industrial process can be used if there is a lack of sufficient protections[9].

http://newsweekme.com/shamoon-virus-returns-new-saudi-attacks-4-year-hiatus/

http://www.middleeasteye.net/news/iran-suspected-cyber-attack-saudi-government-networks-1612048349

State Sponsorship of Cyber Attacks

The Shamoon virus attack against Saudi Aramco has been attributed to Iran. US and Israel allegedly designed and used the Stuxnet virus to sabotage Iran's nuclear weapons program. Russia has reportedly launched cyberattacks against several neighboring countries, including Ukraine, Estonia and Georgia.

In a high profile case, the US Intelligence Community has publicly accused Russian President Putin of orchestrating cyberattacks against the US Democratic National Committee and then providing embarrassing disclosures from the stolen emails to the international media. French and German leaders have also accused the Kremlin of using cyberattacks and internet-propelled fake news to swing opinion behind Russian-backed candidates in recent elections.

In some instances, governments combat cyberattacks to enhance prosperity. However, this motivation may be outweighed by a desire to use cyber attacks to further national security interests.[10] In some experts opinion, this contradiction will never go away. There has been little progress towards international agreements on stronger internet standards or efforts to contain global shocks[11].

Ransomware

In 2017, there were 75,000 ransomware attacks in 99 countries, making it one of the broadest and most damaging cyberattacks in history. The majority of the attacks targeted Russia, Ukraine and Taiwan. But U.K. hospitals, Chinese universities and global firms like Fedex (FDX) also reported they had come under assault. Europol said early May that the attack was of an "unprecedented level and requires international investigation." The ransomware, called "WannaCry," locked down all the files on an infected computer and asks the computer's administrator to pay in order to regain control of them. The exploit was developed following a leak of the US National Security Agency's spy tools. The ransomware is spread by taking advantage of a Windows vulnerability that Microsoft (MSFT, Tech30) released a security patch for in March. But computers and networks that hadn't updated their systems were still at risk. In the wake of the attack, Microsoft said it had taken the "highly unusual step" of releasing a patch for computers running older operating systems including Windows XP, Windows 8 and Windows Server 2003. Affected machines have six hours to pay up and every few hours the ransom goes up. Most folks that have paid up appear to have paid the initial $300 in the first few hours[12].

Private Sector Leadership

Software producers need to produce better software that is less susceptible to hacking. Currently, few consequences exist for software having bad security13. There are calls for software producers to be legally liable for faulty software.

Tech firms have an incentive for developing more secure products. They would be big losers if public trust is completely lost and new internet-based technologies becomes doubtful. Governments should help with research grants.

The insurance industry can help companies understand better the threat. According to one industry expert,

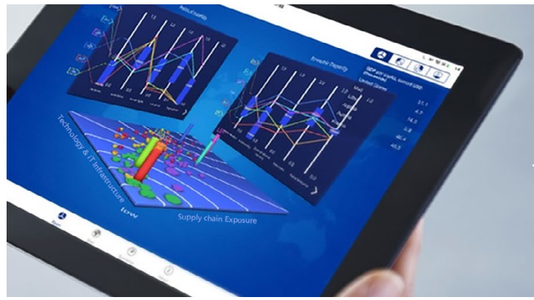
"there are no universally agreed baselines for measuring or managing cyber risk"14. The insurance industry – in assessing the risks facing their clients – should not be focused just on hard- and software deficiencies, but also human factors such as the need for a cyber awareness culture in the workplace.

The private sector along with government need to think through the possible scenarios of IT disruptions and then take preventive actions that can help minimize the risks.

In the case of potential attacks on critical infrastructure such as Smart Grids, the public and private sector can collaborate on information sharing platform to help prevent and respond to the failure of the smart grid, create a sense of principles or "best practices" for risk management practices to apply across the supply chain, develop a liability protocol for cyber looking at what is working well already in other areas (e.g. pools for terrorism, nuclear). In addition, there should be a recognition that risk transfer or finance may not be enough, so that contingency plans at a national level for a serious cyber disaster scenario are in place, incorporating national security agencies (this would be similar to the consequences of a widespread and severe geomagnetic storm). Finally, there should be a public/private sector discussion on what governance principles should apply across a variety of vectors. Among others, it should cover topics such as liability thresholds (who is responsible), duty of assistance (when to intervene), and requirement of cyber insurance.

[7] Ibid.
[8] Ibid.
[9] Ibid., pp. 2-3.
[10] Jay Healey, "A Non-State Strategy for Saving Cyberspace," early 2017. 11 Ibid. Atlantic Council Strategy Series, Number 8, To be Published in early 2017.
[11] Ibid.
[12] http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html.
[13] Ibid.
[14] Paul Nicholas, "Cyber risk and resilience: not understood," Microsoft Secure Blog, October 25 2016, https://blogs.microsoft.com/microsoftsecure/2016/10/25/cyber-risk-and-resilience-not-understood/.

Implications for Risk Management



The Zurich Risk Room (ZRR) is a global risk analysis tool, designed to help illustrate the impact of multivariate risks on individual countries and regions.

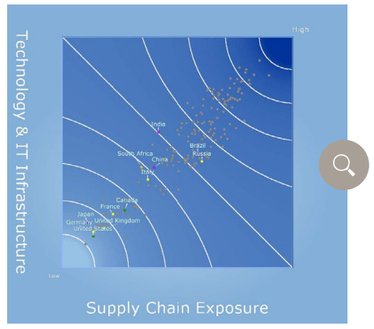
The tool has the ability to look at risks in single dimensions as well as show the complex interactions between many different types of risk.

Increasingly surveys[15] indicate that company executives rate cyberattacks as one of the biggest risks facing companies and societies. Experience shows that at an operational level and often more importantly in terms of its overall business strategy, the C-suite level needs to drive the behavior throughout the organization. Cyber is not only a board and C-suite level issue, it's an enterprise issue that needs to be addressed as an integral part of a holistic risk management strategy.

At a country level, we saw six indicators that bolstered resilience and they all entailed enhancing technology and IT infrastructure including:

- capacity of technology adoption;
- information infrastructure;
- innovation capacity;
- R & D Intensity;
- telecom infrastructure;
- university-industry collaboration in R & D.

On the other side of the risk ledger was supply chain exposure. Better Quality and Quantity of Local Supply and Transport Infrastructure, Logistics Performance, Production Process Sophistication as well as Value Chain Breath and enhanced Financial Market Development would lessen supply chain exposure.

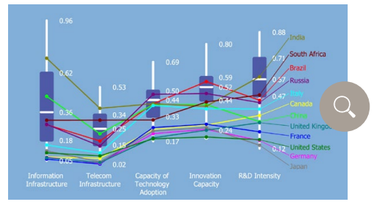


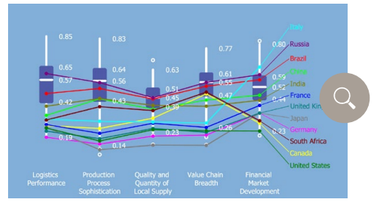
Mapping the supply chain exposure against the technology and IT infrastructure shows which countries are best positioned to deal with cyber risks.

The least risky in the ZRR analysis are Switzerland, United States, Germany, Japan, Sweden and Singapore, but only because companies are taking precautions. High income countries with the most access and use of the internet lose the most from hacking[16]. Germany and The Netherlands were ranked in a 2015 think tank study as suffering the highest losses of any country in the study[17]. But the risk is relatively low because they are investing heavily in cybersecurity. Although preventive measures could be better, governments, publics and companies are increasingly aware of cyber risks.

The BRIC countries stand out among the more developed countries who are at risk. China, India, and Russia have a substantial tech industry but suffer from high levels of corruption and, in the case of China and Russia, are characterized by high levels of cybercrime. There are reportedly 20-30 cybercrime networks in the former Soviet Union with nation-state capability, making cyber defense virtually impossible[18]. Indian companies lose as much as 5% of their profits due to hacking of client information[19]. In Brazil, a third of all Brazilian companies have been victims of cybercrime[20]. Hackers face little legal jeopardy due to "weak laws for cybercrime and intellectual property protection[21]."

The five riskiest countries are all among the poorest in the developing world; Chad, Mauritania, Yemen, Sierra Leone and Burundi. All are listed as among most fragile states in the world by Fund for Peace[22] that track state fragility. None of these countries have any kind of developed tech industry and must rely on outside supply for tech products. An African official has said that "once a country (in Africa) gets broadband connectivity, usually without adequate defenses, cybercrime spikes within a few days[23]."



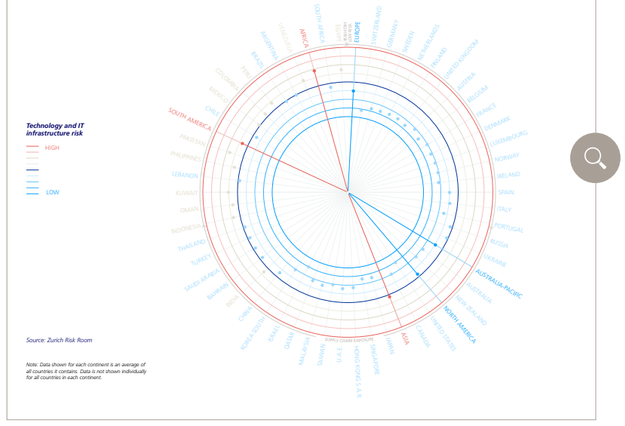


In a Zurich Risk Room scenario on Cyber Security, the BRICS and G7 states above were chosen for illustrative comparison of Technology & IT Infrastructure risks on one side and Supply Chain Exposure on the other side.

According to the World Economic Forum's proprietary Executive Opinion Survey, business leaders in Australia, Canada, Germany, Japan, Singapore, Switzerland, UAE, UK and the U.S. named cyber threat as a top-3 risk to threaten their ability to operate. Companies need to rigorously analyze how these threats could impact their operations and take appropriate risk mitigation and resiliency measures.

https://www.zurich.com/en/knowledge/articles/2017/09/key-data-points-global-risks-of-highest-concern-for-doing-business-in-2017

Cyber risk: Supply chain exposure technology & IT infrastructure



[15] See Zurich's Risks of greatest concern to businesses, Thought Leadership Initiative, September 2017.
[16] Ibid., p. 9.
[17] Ibid., p. 9. CSIS also thought the methodologies that these countries used to calculate cost, along " with difficulties in acquiring information from companies on losses could account for higher than average losses." According to CSIS study, Germany lost 1.60% of GDP on cybercrime; Netherlands 1.50% compared to US at .64% of GDP.
[18] Ibid., p. 15.
[19] "Cyber Crime Warnings for India," BBC, May 6, 2012, http://www.bbc.com/news/business-17979980
[20] Net Losses, p. 8.
[21] Ibid., p. 9.
[22] See Fund for Peace"s website for the latest rankings: http://www.global.fundforpeace.org/index.php.
[23] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," June 2014, p. 6, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

Managing Cyber Risks

Approaches from business continuity management, especially scenario planning, can help with the identification and mitigation of risks. A method to achieve this is Total Risk Profiling® (TRP®). It is a structured approach to identifying, assessing and monitoring risks and improvement actions. Embedding Zurich's TRP® methodology can further help ensure a company's risk management culture is consistent and effective.

TRP® on Cyber Threats – Vulnerability identification

Potential key questions to identify the vulnerabilities related to the cyber scenario, to develop risk scenarios, quantify financial severity and assess probability can be as follows:

1. Vulnerable characteristics of business & organization

- What are risk-sensitive tangible and intangible assets that your board likely agrees to be the most valuable at the heart of your organization's mission? What are the ones your adversaries likely see as most valuable?
- Does your market reputation, image, or brand names expose your company above average? How does your specialization or diversification create a level of attractiveness for cyber attack?
- Do you consider your customers as an interesting target for credit card, data or identity theft?
- How large is your attack surface in terms of technology? Do you see your company as early adopter of new technologies, like Internet of Things (IoT), that are still maturing and are therefore especially vulnerable to attacks and exploits?
- Does your organization operate mainly online and are your products in high demand and completely digital?I Is there a high risk of being infiltrated and robbed of valuable content – both by individuals and organized crime groups?
- How strong is your e-commerce distribution channel directly connected to your company's back-end systems for data processing and supply management, making the website a prime attack point for gaining access to crucial information assets within the organization?
- How experienced at dealing with the challenges of an omni-channel environment is your organization/ your staff?
- How likely is it that your organization is being targeted not only by "traditional attackers" but also by competing companies or even nations engaged in corporate espionage being motivated from money and revenge to competitive advantage and strategic disruption?
- How much is your geographical spread/concentration of doing business exposed to countries with a high cybercrime activity (e.g. Russia or China)?
- How strong is your dependency on subsidiaries/branches that are located in countries with high cybercrime?
- How do your distribution channels/counterparties, especially online ones, create vulnerabilities?
- How dependent are you on bottleneck processes/specific suppliers/Just in Time (JIT) that can be affected by a cyber incident?
- Do you offer safety critical products whose performance can be impacted by a cyber attack?
- Do you operate safety critical processes which integrity or availability can be impacted by a cyber incident?
- How dependent are you on critical infrastructure, alternatively for how long could you be independent?
- Does your business involve build, control and operate critical infrastructure, which could be seen as a target for terrorism, sabotage but also extortion?
- How likely is that disgruntled customers could attack you due to poor complaint handling?
- How likely is it that attackers from inside the company could pose a threat due to poor employee or vendor relations?
- How much has cyber risk been considered in a most recent post-merger/acquisition integration of IT infrastructure?

2. Management style & strategy

- How strong is your governance model in terms of cyber defense?
- Are your management information systems/information technology adequate to the threat?
- Have contract terms been reviewed in terms of so-called "silent" cyber risk clauses that trigger unwanted liabilities based on cyber related incidents?

3. External factors

- How will your stakeholders react to a cyber incident? Specifically:
  - Your shareholders and investors/share price?
  - Your regulator?
  - Your End Users/Customers/Debtors/Creditors?
  - Your Suppliers/Contractors/Partners/Agents/Brokers/ Trade Associations /Utilities?
- How will your image suffer in the eyes of Media/further commentators/watchdogs/general public/society?
- How likely is it that even politics and legislation will react?
- What are possible reaction in the job market, i.e. War on Talent?
- How could competitors use your weakness while being affected by a cyber incident?
- How likely will your creditworthiness be affected in the eyes of banks/suppliers/insurers?

4. Operations & procedures

- How would you rate your threat awareness throughout the organization?
- How advanced is your capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets?
- Do you have a capacity to rapidly contain the damage, and mobilize the diverse resources needed to minimize impact – including direct costs and business disruption, as well as reputation and brand damage?
- Do you know your key employees that are need to be involved in cyber defense?

5. Lifecycle

- Do you apply a comprehensive risk-based lifecycle approach for technologies deployed, which consider cyber risk for implementation, operations, maintenance, end of life, supply chain, support and liability?
- How capable is your organization to quickly adapt to change? Are your cyber resilience capabilities as agile to support the business without hindering time-to-market strategies?

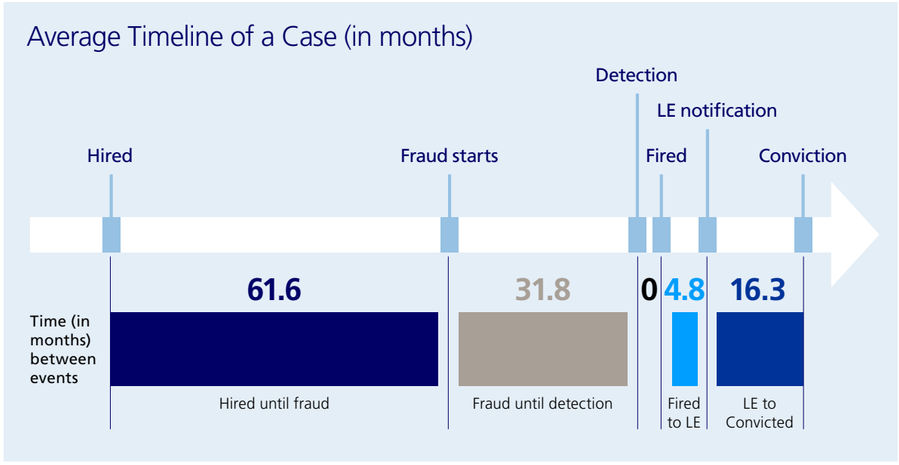
Examples of Intangible assets like intellectual property rights (IP), reputation, compliance. Tangible assets like financial, physical, production systems, infrastructure as well as great goods like safety of life and health, civil liberties, individual privacy.

Other Risk Management Practices

Cybersecurity features high on the agenda of leaders across all sectors. Yet, with the benefits of digitizing and connecting comes a range of new challenges. In response to these challenges, the World Economic Forum recently published an exclusive cyber-risks tool kit to help Board of Directors protect themselves from cyber threats. The report named 'Advancing Cyber Resilience: Principles and Tools for Boards' is a one of a kind innovation tool in the cyber resilience landscape.

The nature of cyber risk is different from others.

- It is harder to establish a firm attribution as to the root cause or culprit than in other criminal categories.
- There are so many different ways a cyber-based system can be vulnerable and fail.
- The fallout of a successful cyberattack is hard to map out ahead of time.
- At the same time, we are increasingly dependent on the internet.
- The gains in efficiency and convenience in the workplace and daily lives make it hard to imagine living without access to the internet.
- For many perpetrators, cybercrime is relatively low risk and low cost while the returns can be large.
- As the costs to businesses and governments increase, it's only recently that we have acknowledged the magnitude of the problem.
- Cyber intrusions are also increasingly used by states in the pursuit of national security.
- Technology players should start thinking of themselves not only as innovators, but also as stakeholders in shaping the future of risk mitigation. With deep technological, data science and related expertise, they have the opportunity and responsibility to take on a larger role in supporting the development of risk mitigation solutions28.



Source: CERT's 2012 Insider Threat Study, p. 26, http://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf.

Companies need to remain agile and alert to the changing nature of cyber threats.

Training employees in basic security practices is a must, and there should be penalties for those who contravene them. Using "predictive analytics" to spot insider threat is evolving rapidly. With social media, it's possible to track not just a person's finances or criminal history, but with whom he/she is associating and his/her state of mind. Tracking of disgruntled employees shouldn't stop when they have been discharged. Some of the costliest cyberattacks occur after a dismissed employee has left the company.

CERT[24], the leading US center on internet security expertise, recommend that managers be trained to spot employees with personal problems, such as high debt levels. In the vast majority of insider cases, legitimate system commands were used in committing the malicious activity. The insiders exploited "known or newly discovered design flaws in systems used to enforce business rules or policies".[25] Practically all of the victims of insider-facilitated crime suffered major financial loss, with amounts ranging from hundreds to hundreds of millions of dollars[26].

Firms need to take measures that mitigate impact of a cyberattack when/if it happens. This includes making backup copies of important business data and information.

Technology players should start thinking of themselves not only as innovators, but also as stakeholders in shaping the future of risk mitigation. With deep technological, data science and related expertise, they have the opportunity and responsibility to take a larger role in supporting the development of risk mitigation solutions. (WEF's Mitigating Risks in Innovative Economy).

As the Internet of Things gets underway, the gaps in protection may not be immediately apparent. Constant testing for potential faults and planning for how to overcome and survive failures will be a must.

With the rapid development of emerging technologies, governments should accelerate the development and use of "regulatory sandboxes" to get ahead of the governance challenge.

The 2008 subprime financial crisis provides some lessons on how to think about cyber risk. To secure themselves, firms need to think beyond their own IT infrastructure and consider six additional aggregations of cyber risk: counterparties and partners, outsourced and contract, supply chain, upstream infrastructure, disruptive tech and external shocks[27].

Finally, all the management consultancies and security firms helping companies deal with the growing threat emphasize the need for top leadership to actively oversee cyber threat prevention.

States, particularly the big powers, need to temper their inclination to see cyber as a tool for hurting opponents. Secure and functioning cyber networks should be seen as advancing prosperity. Governments are in the best position to map out needed measures across industries and for securing critical infrastructures, such as the electric grid.

Investments in technologies and strategies to deter cybercrime should be a priority for both government and business. Too often, we think of cybercrime as the price we pay for doing business using the internet. So long as cybercrime is low risk for the perpetrator, there won't be a way to prevent it.

There is so much at stake if cyber defense isn't strengthened. In the joint Zurich-Atlantic Council study, the Cyber Shangri-La scenario which involved better defense yielded 10% more in terms of cumulative GDP out to 2030. If the Internet of Things is to be implemented and not sidetracked, public trust in the internet has to be strong.

Just as protecting sea lanes has been important for centuries in nurturing for trade and commerce, the internet is now part of that same global commons that governments and the private sector have a responsibility to protect.

[24] CERT stands for Center of Internet Security Expertise which was established by Department of Defense and operates out of Carnegie Mellon University in Pittsburgh, PA.
[25] "Insider Threat Study: Illicit Cyber Activity Involving Fraud in US Financial Sector," July 2012, CERT, p. 17, http://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf.
[26] "Insider Threat Study: Illicit Cyber Activity Involving Fraud in US Financial Sector," July 2012, CERT, p. 17, http://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf.
[27] Jason Healey, "Beyond data breaches: global interconnections of cyber risk," Atlantic Council, April 2014, https://www.zurich.com/_/media/dbe/corporate/docs/whitepapers/risk-nexus-beyond-data-breaches-global-interconnections-of-cyber-risk-2014.pdf.
[28] http://www3.weforum.org/docs/WEF_Mitigating_Risks_Innovation_Economy_report_2017.pdf, p.6.

Disclaimer

This publication has been prepared by Zurich Insurance Group Ltd and the opinions expressed therein are those of Zurich Insurance Group Ltd as of the date of writing and are subject to change without notice.

This publication has been produced solely for informational purposes. All information contained in this publication have been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Group Ltd or any of its subsidiaries (the 'Group') as to their accuracy or completeness.

This publication is not intended to be legal, underwriting, financial, investment or any other type of professional advice. The Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this publication. Certain statements in this publication are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors.

The subject matter of this publication is also not tied to any specific insurance product nor will it ensure coverage under any insurance policy.

Zurich Insurance Company Ltd
Mythenquai 2
8002 Zurich
Switzerland

173004111 (11/17) TCL

ZURICH®