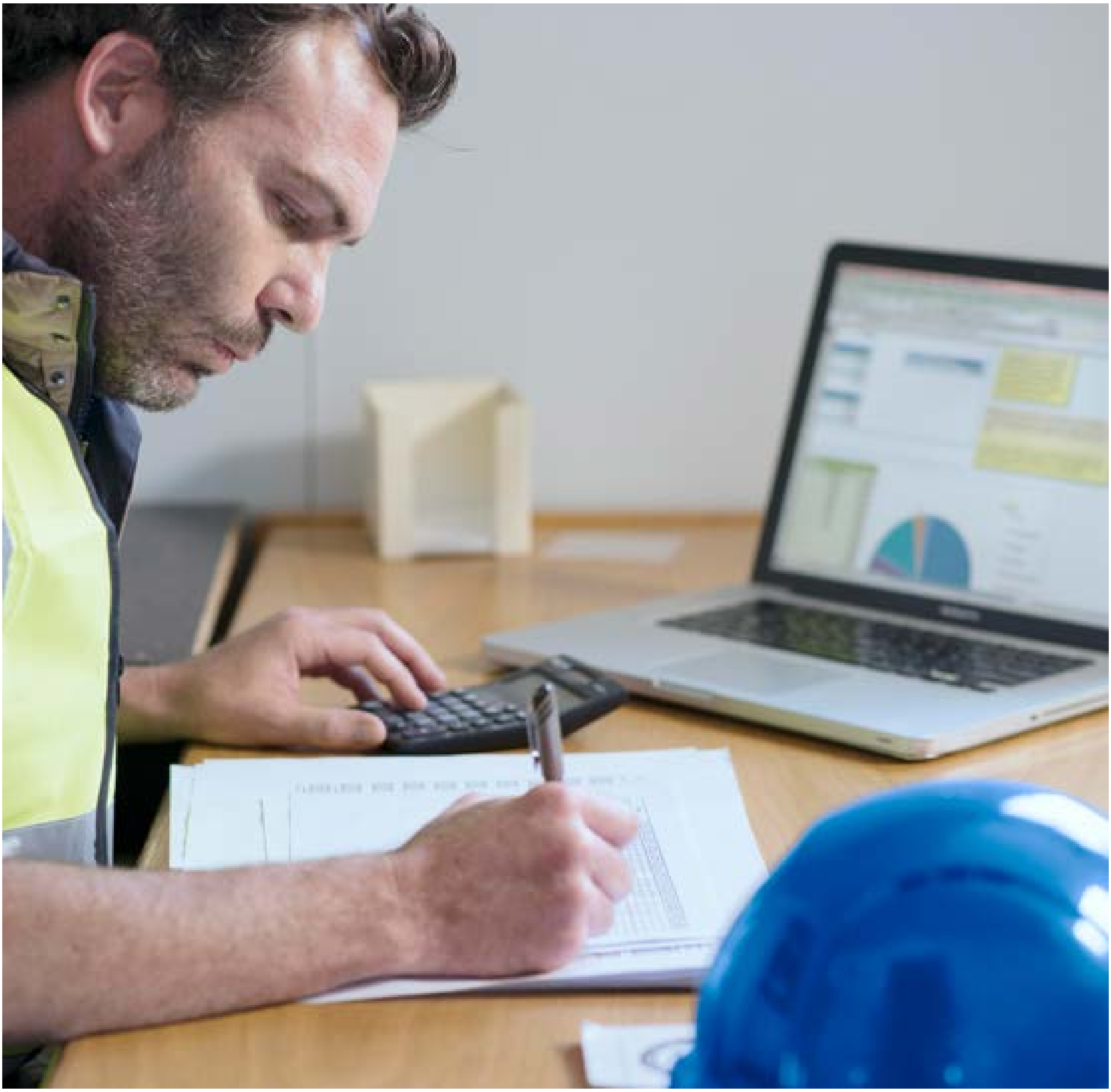
ZURICH®

Cyber security and the construction industry

Staying ahead of emerging threats



Foreword

In our increasingly digitized world, cyber risk is an important issue for all businesses to understand and manage. We look at the risks facing the construction sector and how it can stay ahead of emerging cyber threats.

The construction industry deals primarily in the tangible. This can make it difficult for organizations to fully appreciate the true nature and scale of seemingly intangible risks – such as cyber threats and cyber attacks.

However, the sector is far-from immune to cyber threats, managing vast amounts of critical service data and information that is very attractive to cyber criminals.

Technology is progressively permeating all aspects of construction operations. From the digital tools used at design stage, to the laptops and smartphones we all use to communicate and access key information – technological change is progressing on a daily basis.

While the industry's principal focus will always be on the physical, as the world becomes increasingly digital, it is important for all construction sector organizations to get to grips with this important area of risk.

Bernadette Hackett
Global Relationship Leader
Head of the Global Construction Industry Community
Zurich Insurance plc

Nikki Ingram
Cybersecurity Risk Engineering
Risk Engineering
Zurich North America

Matia Cazzaniga
Global Head of Engineering Lines and Construction
Zurich Commercial Insurance

A new world

Cyber security is a growing challenge for individuals, businesses and governments. Our increasingly connected world may present exciting opportunities, but it is also introducing new risks for construction firms to deal with.

Revolutionary times

We stand on the brink of the Fourth Industrial Revolution, according to the World Economic Forum – innovating at an exponential and unprecedented rate, and inspiring a "fusion of technologies that is blurring the lines between physical, digital and biological spheres".

There are now more objects connected to the internet than there are people on the planet, demonstrating the extent to which technology permeates our everyday lives.

Businesses are typically early adopters of new technology, and the construction industry is no exception. Innovations, ranging from brick-laying robots to the humble smartphone, have quickly found their way onto project sites across the globe.

While such technologies have the potential to greatly improve firms' capabilities and operations, they also present new avenues of attack for cyber criminals.

Growing awareness

Cyber risk has shot up the global agenda in recent years, following a wave of high-profile data breaches. Successful attacks against tech giants such as Google and Sony show us the sophistication of today's criminals, while 2017's WannaCry ransomware strike highlights the often-untargeted nature of attacks, and the fact that no one is immune.

With the average cost of a data breach currently sitting at $3.62m, according to research by IBM and the Ponemon Institute, cyber security is of increasing concern for today's businesses, and a key strategic risk to manage.

However, while awareness of these risks is certainly growing, many construction firms have been slow to properly identify and address their full range of vulnerabilities.

As the world becomes progressively digitized and connected, it is important that every business keeps pace with it, taking proactive steps to safeguard against emerging threats.

Cyber attacks are not limited to data breaches, but also include business interruption and even physical harm. Only severe cases make it to the news because there are not the same reporting requirements as there are for data-breach incidents.

WannaCry

- The ransomware encrypted victims' data and demanded a ransom to decrypt and restore access to their systems and data
- It exploited a security vulnerability on older editions of Microsoft Windows
- Within one day, it had infected more than 230,000 computers in over 150 countries, going on to infect over 400,000 worldwide
- Victims included the UK's National Health Service (NHS), Deutsche Bahn and FedEx
- French construction-materials firm Saint-Gobain was impacted by a similar attack by 'Petya' ransomware in 2017

USD
3.62m
average cost of a data breach

IBM, Ponemon Institute, 2017 Cost of Data Breach Study

Risks facing the construction industry

Construction firms rarely hold large amounts of sensitive personal data, such as customer credit-card information, but this is no reason to be complacent. The sector is still ripe with information and opportunities that are appealing to cyber criminals.

Tip of the iceberg

When a cyber attack makes the headlines, it usually concerns sensitive personal data such as personally identifiable information or credit-card information. A growing body of legislation exists regarding personal data, with many jurisdictions requiring notification to authorities and data subjects should a breach occur. Stories of personal data breaches therefore naturally receive the greatest exposure.

However, personal data is just the tip of the iceberg. Enormous value exists in other types of data, and cyber criminals are rarely fussy about what they steal or where they steal it from. Non-personal data is seldom subject to the same notification requirements and, since no one wishes to air their dirty laundry in public, the vast majority of cyber attacks are not publicized.

Valuable information

The construction industry holds vast amounts of information that is of interest to cyber criminals – from employee data to intellectual property – all of which can be potentially exploited for financial gain or other motives.

For example, should someone gain access to the design files for a bridge under construction, changing a single measurement could drastically alter its load-bearing capacity. The organization could then be held to ransom in return for details of what the attacker has altered. The attacker may not understand the potential impact of what they have done, though in extreme cases their goal may be to cause the structural failure of the bridge.

Motivations other than money

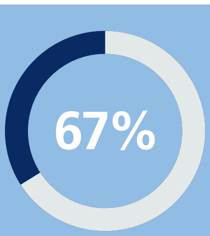
Data is not the only target, nor monetary gain the only motive. A report by the Information Systems Audit and Control Association (ISACA) found that only half of cyber attacks were in fact motivated by financial gain.

Today's organizations are exposed to a much wider spectrum of potential attacks, from disruption of services to state-sponsored cyber warfare. For example, in 2013, an Australian building contractor made the headlines when a Chinese hacker stole blueprints to the new headquarters of the Australian Security Intelligence Organization (ASIO).

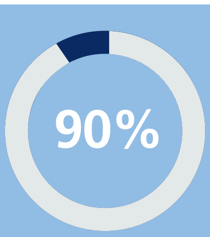
When you consider how many functions now have a digital element – from office payroll systems to equipment being used on site – there is an increasing number of avenues for attackers to exploit, thanks to this burgeoning Internet of Things.

> “If you haven't suffered a data breach, you've either been incredibly well prepared or very, very lucky. Are you incredibly well prepared?”

Verizon, 2017 Data Breach Investigations Report



of cyber incidents went unreported



of incidents were preventable

Online Trust Alliance, 2017 Cyber Incident & Breach Readiness Guide

Damage and interruption

Attacks in the digital world can have serious consequences for an organization's physical assets and business continuity. However, historically, neither customers nor the insurance industry have fully understood the importance and scale of this interaction, leading to limited loss data and a lack of general awareness.

For example, a customer experiences a loss from a mechanical fire where a machine overcharged due to a temporary failure in the automated control system. A claim is made for physical damage and business interruption, but investigations do not extend to the root cause of the system's temporary failure, and whether there was any element of cyber interference.

While incidents such as this aren't common, they can be very serious, leading to severe consequential damage and business-interruption losses. Organizations carrying out activities that support a country's strategic infrastructure, such as energy and transport, tend to face a greater risk of such an attack, both in terms of likelihood and severity.

With a growing number of physical assets connected to a company's network, there is no longer a clear dividing line between the physical and the digital. It is therefore important to appreciate cyber risk's ability to cross such barriers, and to consider this when both managing potential risks to physical assets and examining losses. Choosing the right insurance partner is crucial in order to have easy access to the level of expertise required to navigate this challenging area or risk.

> "We need to raise awareness of these physical exposures. It's not a matter of frequency; it's a matter of severity."
>
> Matia Cazzaniga, Global Head of Engineering Lines at Zurich

Digital to physical – case studies

Zurich is part of an industry-wide working group exploring the threat of cyber risk to cause physical damage and consequential loss.

The group's latest white paper includes a wealth of helpful information for construction organizations, including numerous real-world case studies.

Read more at: **IMIA - The International Association of Engineering Insurers**

Offline focus

Construction firms' primary focus is offline, dealing with buildings, infrastructure and other tangible resources. It is therefore understandable that digital assets do not always receive the same attention as they might in other industries.

With the majority of incidents going unreported, and no industry-wide practice of reporting or sharing incident details, it is difficult for construction organizations to learn from each other's mistakes and collectively improve cyber security across the sector.

Businesses that you might not consider a typical target are increasingly falling victim to attacks, as many lack the necessary controls to mitigate cyber risk. Construction firms can therefore represent low-hanging fruit for cyber criminals, with common vulnerabilities witnessed throughout the industry.

Proactive defenses

All construction firms need to be proactive with cyber security and take a broad view in addressing their vulnerabilities. This encompasses:

- Physical controls – for example, locking screens on unattended devices and controlling access to areas where sensitive information could potentially be accessed.
- Technical controls – for example, ensuring machines have the latest updates, security patches and encryption methods, and tools like firewalls and antivirus.
- Administrative controls – for example, policies and procedures, and training employees, contractors and sub-contractors on their role in maintaining information security.

Nowadays, with something as simple as a printer offering a potential door into an organization's entire network, anything that either stores data or has a connection to the outside world needs to be examined from a cyber-security perspective.

Common vulnerabilities

- Lack of employee training
- Older operating systems
- Slow security patching
- Weak login credentials
- Physical theft on site
- Phishing scams
- Unencrypted communications

Protecting your organization

In an increasingly digitized and connected world, cyber security needs to be considered at all stages of a firm's operation. While it may seem daunting, cyber security can be approached in the same way as you would any other risk.

Keep informed and stay ahead

Cyber criminals are continually evolving, modifying their techniques to sidestep defenses and exploit new avenues of attack. The construction industry needs to be equally proactive in its response, looking at the risks holistically and instilling a genuine culture of cyber security in the boardroom, on site and everywhere in between.

Governments across the globe are increasingly legislating on the issue, placing higher standards on how businesses must protect and manage their information. To avoid the pressures of playing catch-up to achieve compliance, businesses should act now to establish a sensible approach to cyber risk. As laws and regulations continue to emerge, so fine-tuning to meet specific requirements will become much more manageable.

As cyber risk grows, it ultimately threatens to outweigh the benefits that construction firms gain from technological advances. Proactively addressing the associated risks will help organizations continue to reap the benefits of greater digitization and connectivity.

Not just an IT issue

Crucially, cyber risk should not be seen as an issue solely for your IT department or provider. While IT infrastructure is an important factor in managing cyber risk, it is just one piece of a much larger puzzle. IT professionals are primarily focused on network functionality, whereas cyber risk is a much broader issue, affecting all aspects of an operation – from how you deal with third parties to the actions of frontline staff.

Cyber risk is a major strategic risk, demanding board-level attention and requiring input from all departments.

Framework for success

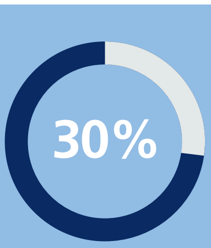
It is important for modern businesses to appreciate the likelihood that they will fall victim to some form of cyber threats and cyber attacks. Once cyber is accepted as a key strategic risk, organizations can progress to not only protect themselves, but plan how they will respond and recover when an incident occurs.

Cyber risk is a complex topic that permeates all levels of an organization, making it challenging to comprehend and tackle effectively. To enable everyone to understand their role and take meaningful action, the National Institute of Standards and Technology (NIST) in the United States has developed a helpful five-point framework.

The NIST framework offers a comprehensive, flexible and easy-to-understand template for managing cyber risk, and is the preferred method of many cyber-security experts. For full information, visit: www.nist.gov/cyberframework

> "Think of bad weather, like a snow storm. Those who have prepared tend to suffer little disruption. Cyber risk is no different – basic preparations make the difference between an inconvenience and a crisis."

Nikki Ingram, CISSP, Cyber Security Risk Engineer at Zurich



30% of US companies currently use the NIST framework to manage their cyber risk.

By 2020, this is expected to increase to 50%

National Institute of Standards and Technology

NIST framework

1.Identify

- Identify what is most critical to the running of your organization – from the information you hold to key activities and processes
- Risk assess all IT assets – software, hardware and data
- Classify assets according to their role in the running of your organization and their level of exposure to cyber attacks

2.Protect

- Prioritize action for those assets identified as most in need of protection
- Start with basic protections, of physical, technical and administrative nature

– Physical: including storage locations, physical barriers, screen-locking and personnel access

– Technical: including encryption, network segmentation, security patching, passwords, access privileges and endpoint protection tools

– Administrative: including policies, procedures, standards and staff training

- Establish more sophisticated and targeted protection for your most sensitive or at-risk assets

3.Detect

- Establish a means of continually testing that your protective controls are functioning and that procedures are being followed by staff and partners
- Recognise when protective controls have failed or have been bypassed as an early warning of a potential attack
- Have effective means of knowing when a cyber attack is occurring

4.Respond

- Theorize different types of breach, and plan precisely how you would respond to different scenarios
- Ensure that you have the capacity to continue defending against other attacks while responding to a particular security breach
- Periodically test and refine your response plans

5.Recover

- Plan how to minimize the impact of a breach and recover quickly
- Regularly back-up critical data and have the ability to establish a clean computing environment

Familiar thinking

Using the example of fire risk, we can see how the framework helps to manage any type of risk. This makes it simple for everyone within an organization to understand and play their part.

Fire risk – NIST process

- Identify what could catch fire and how that might occur – such as the risk of open flames when working around combustible building materials
- Protect against such risks, whether that's by establishing safer operating procedures or by increasing the presence of fire extinguishers on site
- Detect fires when they occur by installing appropriate monitoring and alarm systems
- Respond to an incident quickly and effectively, creating and regularly testing formal evacuation and response procedures
- Recover swiftly by planning in advance for potential scenarios, and making preparations that will minimize the impact to the organization

How can we help?

Our expert Risk Engineers can help you to identify the risks you face and develop effective strategies to secure the continued success of your business.

Reducing costs

Our Risk Engineering approach is focused on helping you to understand and manage cyber risk, and to minimize the impact of a cyber event. Cyber attacks not only have direct financial consequences, they can also have an array of associated costs – from reputational damage to lost business opportunities.

Our Risk Engineers will look at your organization through a broad lens, helping you to understand the full range of exposures you face and the best strategies to manage them.

Impartial advice

We offer candid, impartial advice on the best means of tackling cyber risk. While other providers can sometimes be biased towards particular technologies and services that they supply, we will always remain neutral and recommend the best course of action for your particular needs.

Industry knowledge

Our Risk Engineering team benefits from a wide range of industry knowledge and expertise, enabling us to better understand and serve our clients.

Many of our Risk Engineers have previously worked in the construction sector and its associated trades, offering unrivalled insight into your activities and the challenges you face.

Beyond cyber

Our Risk Engineering expertise extends far beyond cyber risk, delivering a range of services to the construction sector, such as:

- Construction professional indemnity site survey
- Quality management systems check
- Subcontractor default risk analysis
- Temporary works management review
- Tunneling works management and construction site survey
- Construction site water damage risk mitigation review and advice
- Timber-frame construction fire mitigation review and advice

Find out more

For more information on how we can help your business:

Visit: **www.zurich.com**

Email: **risk.engineering@zurich.com**

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 has 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 its 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. This publication may not be distributed or reproduced either in whole, or in part, without prior written permission of Zurich Insurance Group Ltd, Mythenquai 2, 8002 Zurich, Switzerland. Neither Zurich Insurance Group Ltd nor any of its subsidiaries accept liability for any loss arising from the use or distribution of this publication. This publication does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction. www.zurich.com