Allianz

CYBER INSIGHTS

Ransomware trends: Risks and Resilience

Allianz Global Corporate & Specialty

About AGCS

Allianz Global Corporate & Specialty (AGCS) is a leading global corporate insurance carrier and a key business unit of Allianz Group. We provide risk consultancy, Property-Casualty insurance solutions and alternative risk transfer for a wide spectrum of commercial, corporate and specialty risks across 10 dedicated lines of business.

Our customers are as diverse as business can be, ranging from Fortune Global 500 companies to small businesses, and private individuals. Among them are not only the world's largest consumer brands, tech companies and the global aviation and shipping industry, but also satellite operators or Hollywood film productions. They all look to AGCS for smart answers to their largest and most complex risks in a dynamic, multinational business environment and trust us to deliver an outstanding claims experience.

Worldwide, AGCS operates with its own teams in more than 30 countries and through the Allianz Group network and partners in over 200 countries and territories, employing around 4,400 people. As one of the largest Property- Casualty units of Allianz Group, we are backed by strong and stable financial ratings. In 2020, AGCS generated a total of €9.3 billion gross premium globally.

www.agcs.allianz.com

Introduction

Cyber intrusion activity globally jumped 125% in the first half of 2021 compared with the previous year, according to Accenture[1], with ransomware and extortion operations top two contributors behind this triple-digit increase. There is little evidence that ransomware attacks show any sign of letting up. Weak cyber security, challenging conditions for law enforcement and cryptocurrencies are creating fertile ground for criminals, who continue to find lucrative rewards with little risk of prosecution.

The frequency and severity of attacks has escalated in the past two years. According to the Federal Bureau of Investigation (FBI)[2] there was a 62% increase in ransomware incidents through the first six months of 2021 in the US, which followed a 20% increase in the number of incidents for the whole of 2020 and a 225% increase in ransom demands. Globally, across 2021 ransomware attacks are estimated to cost businesses around $20bn, according to Cybersecurity Ventures[3], a total predicted to reach $265bn by 2031.

Ransomware has become a real menace for businesses across all sectors. And with no easy remedy in sight, the onus is on individual companies to invest in cyber security and make life harder for gangs. Those companies that take steps to prevent attacks and mitigate the impact will be far less likely to fall victim to ransomware.

"The number of ransomware attacks may even increase before the situation gets better. As insurers we have to continue to work with our clients using a combination of policy and service improvements to help businesses understand the need to strengthen their controls," says **Scott Sayce, Global Head of Cyber at AGCS and the Global Head of the Cyber Center of Competence for AGCS and the Allianz Group.** "Not all ransomware attacks are targeted. Criminals also deploy wild scattergun approaches to exploit those businesses that aren't addressing or understanding the vulnerabilities they may have.

"In today's rapidly evolving market for cyber insurance coverage, providing the emergency response services, as well as financial compensation, in the wake of the numerous different types of cyber-attacks is now the standard. The cyber insurance market is providing the 'digital SWAT team' in addition to the covered financial losses."

> There is little evidence that ransomware attacks show any sign of letting up

1 Accenture, Global Cyber Intrusion Activity More than Doubled in First Half of 2021, According to Accenture's Cyber Incident Response Update, August 4, 2021
2 FBI, Ransomware Awareness for Holidays and Weekends, August 31, 2021
3 Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031, June 3, 2021

From $40 a month subscription – ransomware as a business

Cyber extortion, and ransomware in particular, has become big business. Attacks have increased as criminals have become more organized, refining their tactics and business models. The development of **'ransomware as a service' (RaaS)**, for example, has made it easier for criminals to carry out attacks. Run like a commercial business, RaaS groups like REvil and Darkside sell or rent their hacking tools to those who carry out the attacks and extort victims. They also provide a range of support services, including helplines and ransomware negotiation services.

RaaS has lowered the barriers to entry and enabled criminals to scale up their efforts and ramp up their attacks. Even those with little technical knowledge can launch ransomware attacks using RaaS. From as little as a $40 per month subscription, successful attacks can yield many thousands of dollars from ransomware payments. REvil, may have collected close to $100mn in ransom payments in just the first six months of 2021, according to estimates[4].

Ransomware gangs are fundamentally driven by commercial motivations, such as efficiency and profitability, explains **Michael Daum, Senior Cyber Underwriter at AGCS:** "Ransomware is run like a business. All the trends we see, such as the significant increase in the number of groups deploying 'double extortion' attacks, the surge in supply chain incidents (and even the emergence of 'triple extortion') *(see page 9)* are all just ways in which criminals are seeking to increase their return on investment and their efficiency, optimizing their attacks in order to get the best outcome."

4 Coveware, Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority, July 23, 2021

More threat actors, more attacks, more claims

The combination of high rewards and low risk for cyber criminals means that ransomware is here to stay, at least for the foreseeable future, according to **Marek Stanislawski, Global Cyber Underwriting Lead at AGCS.**

"The knowledge threshold to carry out attacks is relatively low and ransomware tools are more easily accessible. Together with cryptocurrencies *(see box, right)* and the relative ease with which gangs can avoid detection and prosecution, ransomware is an area where criminals can easily thrive."

Our increasing reliance on digitalization, the surge in remote working following Covid-19, and IT budget constraints are just some of the reasons why IT vulnerabilities have intensified and there are now countless numbers of access points for criminals to exploit. Initial attacks are typically automated, with many cyber gangs previously limited by the human capacity required to follow up on attacks. However, that capacity has been increasing as gangs have invested in additional resources, Stanislawski notes.

"Now, there are many more malicious threat actors on the scene, while criminals are using ever more aggressive tactics to extort money," says Stanislawski. "This has helped drive up the frequency and severity of ransomware attacks and claims in recent years."

Losses resulting from external incidents, such as Distributed Denial of Service (DDoS) attacks and ransomware campaigns, account for the majority of the value of cyber claims (81%) analyzed by AGCS over the past six years. There has been an increase in ransomware incidents over the past two years in particular, with the number of claims rising by 50% year-on-year in 2020 (90). The total of ransomware claims received in the first half of 2021 is already the same as reported during the whole of 2019 (60), although this still represents a relatively small proportion of claims overall.

The cryptocurrency factor

Cryptocurrencies are an important part of the ransomware business model, and one of the drivers behind the growth in this illicit market. Cryptocurrencies like Bitcoin (which is estimated to account for approximately 98% of ransomware payments[5]) are relatively easy to acquire and use, while payments are verifiable. Transactions can also be carried out with anonymity, enabling perpetrators to keep their identities hidden.

"Cryptocurrencies are a key factor in the rise of ransomware – it's what makes it straightforward. They are the weak link that enables criminals to bypass traditional institutions and hide behind the anonymity built into the technology. More stringent enforcement and compliance with 'know-your-customer' and anti-money laundering laws could, however, help disrupt the ransomware business model," says **Thomas Kang, Head of Cyber, Tech and Media, North America at AGCS.**

5 Coveware, Ransom amounts rise 90% in Q1 as Ryuk increases, April 16, 2019

Changing tactics

> The majority of ransomware attacks are not targeted, nor are they technically sophisticated

Recent years have seen growth in the use of **'double extortion'** tactics, whereby cyber criminals combine the initial encryption of data with a secondary form of extortion, such as the threat to release sensitive or personal data. Hackers will also now attempt to encrypt or delete backups, making restoration and recovery more difficult or impossible. A worrying recent trend has seen attackers harass employees to gain access to systems, as well as go directly to company senior executives to demand ransoms.

Sophisticated targeted cyber-attacks are typically the work of a small number of highly-resourced (and often state-supported) hacking groups, as well as foreign intelligence services.

Such attacks typically use 'zero-day' exploits – previously unknown bugs in software – to infiltrate systems and steal data without being detected. In contrast, the vast majority of ransomware attacks are the work of criminal gangs, motivated by financial reward, according to **Thomas Kang, Head of Cyber, Tech and Media, North America at AGCS.**

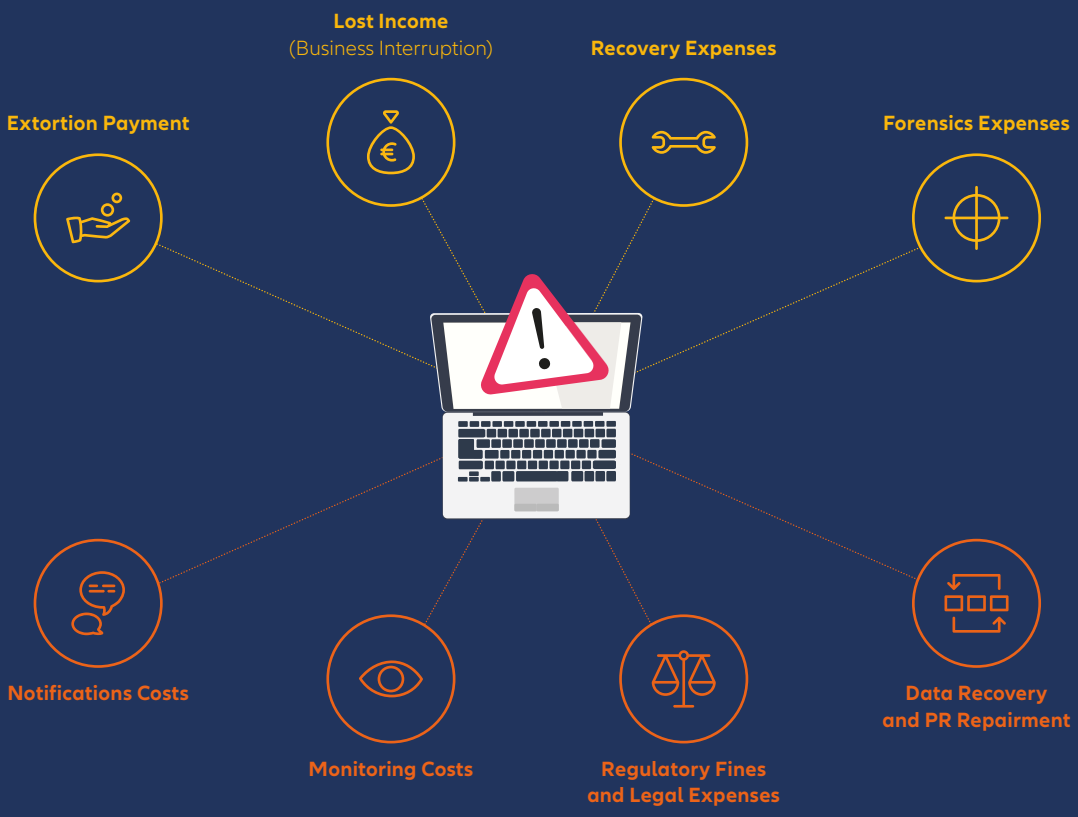
"We often hear about high-profile sophisticated attacks in the media, but as a whole the majority of ransomware attacks are not targeted, nor are they technically sophisticated," says Kang. "For the most part cyber criminals are looking for the most vulnerable firms, focusing their efforts on where there is the best chance of receiving a pay-out for the least effort."

Cyber risk modeling firm Kovrr[6] researched a double digit number of active 'double extortion' ransomware attack campaigns over a year. Of the campaigns studied, 75% used social engineering (phishing emails) to propagate, while 25% of them involved exploiting a vulnerability in remote access software.

6 Kovrr, Key Drivers of Rise of Ransomware in 2020, February 2021

Ransomware costs – double extortion changes the rules and multiplies the cost

Potential costs from a 'conventional' ransomware attack
(which encrypts the attacked company's data without leaking it)



Potential **additional** costs from a ransomware attack which becomes **a data breach event**
(stealing and then publishing the data)

Costs description:

Single Extortion

Extortion Payment: demanded by criminals

Lost Income (Business Interruption): The longer period of time in which system accessibility is limited, the greater the loss.

Recovery Expenses: the cost of restoring data and ensuring full systems recovery.

Forensics Expenses: expenses incurred to investigate the source of the security vulnerability.

Double Extortion

Notifications Costs: notifying customers, regulators and other required authorities of a data breach.

Monitoring Costs: monitoring services for identity theft/ fraud that has to be supplied to individuals whose data is stolen.

Regulatory Fines and Legal Expenses: due to third parties' claims whose private data is stolen.

Data Recovery and PR Repairment: Costs of a consultant, crisis management firm or law firm to limit effects of negative publicity.

Sources: Bitsight and Kovrr. Graphic: Allianz Global Corporate & Specialty.

Supply chain attacks expected to increase

High-profile ransomware attacks in the past year point to emerging trends, notably an increase in supply chain attacks.

There are two main types – ones that target software/IT service providers and use them to spread the malware and ones that target physical supply chains, such as critical infrastructure.

For example, the ransomware attack against the Colonial Pipeline[7], the largest cyber-attack on US oil infrastructure to date, caused a week-long disruption to fuel supplies on the US east coast in May 2021. Colonial paid the $4.4mn bitcoin ransom in order to restore its systems, although some $2mn was later recovered. According to the FBI[8], cyber criminals are increasingly targeting large, lucrative firms and providers of critical services with the expectation of higher-value ransoms and increased likelihood of payments.

7 Bloomberg, Hackers Breached Colonial Pipeline Using Compromised Password, June 4, 2021
8 FBI, Ransomware Awareness for Holidays and Weekends, August 31, 2021

What is triple extortion?

The success of double extortion as a form of cyber-attack since the beginning of the Covid-19 pandemic demonstrates how the ransomware threat continues to evolve. The next challenge to overcome? Triple extortion...

Ransomware attacks globally surged by more than 100% during the first half of 2021 compared with 2020, according to Check Point Research[9], a software technologies company, fueled by innovation in a new attack technique called triple extortion.

With triple extortion ransomware, hackers combine three forms of attack – DDoS, file encryption and data theft – and don't just target one company.

The first notable case was the Vastaamo clinic attack[10], which happened in October 2020. The 40,000-patient Finnish psychotherapy clinic suffered a year-long breach that culminated in extensive patient data theft and a ransomware attack. A ransom was demanded from the clinic, but smaller sums were also demanded from the patients, who received the ransom demands individually by email. The attackers threatened to publish therapist session notes unless ransoms were paid.

Increasingly, hackers are also using digital supply chains to launch ransomware attacks. Earlier this year, REvil infiltrated the systems of software provider Kaseya, injecting ransomware into an update sent out to the firm's managed service provider (MSP) clients, who then unwittingly exposed their own customers. The attack resulted in one of the largest, and most unusual, ransom demands to date. REvil offered to provide a universal decryption key that would unlock the data and systems of all affected firms in return for a one-off payment of $70mn. Kaseya[11] says it did not pay the ransom.

The attack followed a similar incident involving US technology company SolarWinds, whereby hackers compromised the firm's software in order to access thousands of companies and government offices that used SolarWinds products.

In a similar vein, in March 2021, 'zero-day' vulnerabilities in Microsoft Exchange[12] Server software were initially exploited by suspected nation-state hackers but have since been used by groups taking advantage of the vulnerabilities in unpatched servers to launch ransomware attacks.

"Supply chain attacks are likely to be the next big thing in ransomware," says Stanislawski. "I suspect we will see more attacks like against Kaseya. There are many companies like Kaseya that supply thousands of businesses, and offer opportunities to wreak damage with the chance of a higher payout. This makes them prime targets."

Indeed, the European Union Agency for Cybersecurity (ENISA[13]) projects that supply chain attacks will quadruple by the end of 2021 compared to last year.

The ransomware attack against the Colonial Pipeline, the largest cyber-attack on US oil infrastructure to date, caused a week-long disruption to fuel supplies on the US east coast in May 2021

9 Checkpoint Software Technologies, The New Ransomware Threat: Triple Extortion
10 Wired, A dying man, a therapist and the ransom raid that shook the world, December 9, 2020
11 Bloomberg, Kaseya Says It Didn't Pay a Ransom To Hackers, July 26, 2021
12 CSO, The Microsoft Exchange Server hack: A timeline, May 6, 2021
13 ENISA, Threat Landscape for Supply Chain Attacks, July 29, 2021

$5.3mn

The average extortion demand in the first half of 2021

$570,000

The average payment in the first half of 2021

Ransom dynamics

Ransom demands have rocketed over the past 18 months. According to cyber security firm Palo Alto Networks[14], the average extortion demand was $5.3mn in the first half of 2021, a 518% increase on the 2020 average. The highest demand was $50mn, up from $30mn last year, according to the firm, however, the amount paid to hackers is often much lower. Average payments were $570,000 in the first half, up 82% from 2020.

Law enforcement agencies typically advise against paying extortion demands, which is thought to fuel the problem and potentially incentivize further attacks in the future. Paying a ransom is also not a guarantee that a business will be able to quickly retrieve its files and restore its systems. In many cases, by the time the ransom is paid, the damage is already done, and most organizations will have already suffered loss of income and incurred the expense of restoring files and systems.

"Even when a company pays a ransom, it takes a huge effort to restore files and get systems back up and running. This is a huge undertaking, even when you have a decryption key," says Stanislawski.

Attacks like the one against the Colonial Pipeline have helped turn up the political heat for ransomware gangs. As a result, there have been calls to ban the payment of ransoms, or at least require companies to report ransom payments, although these are subject to applicable laws and regulations and the issue becomes even more complex in cases which may involve threats to life. In any case, the impacted company should inform and cooperate with the police or national investigation authorities.

14 Palo Alto Networks, Extortion Payments Hit New Records as Ransomware Crisis Intensifies, August 9, 2021

Business interruption and recovery costs main drivers of ransomware losses

Business interruption losses and restoration costs are the biggest driver for ransomware losses, as they are for most losses from cyber incidents, AGCS claims analysis shows *(see box)*.

The average total cost of recovery and downtime from a ransomware attack more than doubled over the past year, increasing from $761,106 in 2020 to $1.85mn in 2021, according to the State of Ransomware report[15]. Average downtime following a ransomware attack is 23 days[16].

"When it comes to cyber business interruption, timing is everything. If you pay a ransom demand after a week, the loss has already crystalized and the cost of restoration is already set in motion. For example, the cost of hiring forensic experts and response consultants can run to $2,500 per day and easily reach a seven-digit figure," says **Rishi Baviskar, Global Cyber Experts Leader, Risk Consulting, AGCS.**

15 Sophos, State of Ransomware 2021, April 27, 2021
16 Coveware, Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority, July 23, 2021

A steady increase in cyber claims

The number of cyber insurance claims AGCS has seen has steadily increased in recent years, including notifications of ransomware attacks, driven in part by the growth of the global cyber insurance market. During 2020, AGCS received more than 1,000 cyber-related claims in total compared with around 80 in 2016 when cyber was a relatively new line of insurance. This trend has continued in 2021 with more than 500 cyber claims received in the first half of the year.

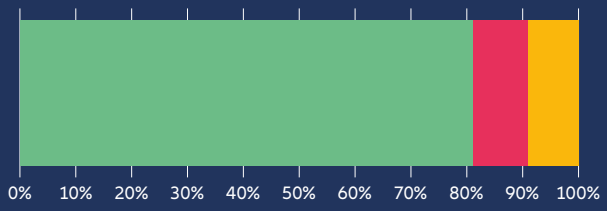
Losses resulting from external incidents, such as DDoS attacks and including ransomware campaigns, account for the majority of the value of cyber claims (81%) analyzed over six years. There has been a jump in ransomware incidents over the past two years with the number of claims increasing 50% year-on-year in 2020 (90). The total reported in the first half of 2021 is already the same total as reported during the whole of 2019 (60), although this still represents a relatively small proportion of claims overall.

Nevertheless, numerous industries and sectors have been impacted including hospitals/ healthcare, retail, cosmetics, technology and communications, distribution and logistics companies, construction, and cloud computing service providers.

Business interruption is the main cost driver behind cyber losses, accounting for well over 50% of the value of close to 3,000 insurance industry cyber claims worth around €750mn ($885mn).

"The claims environment and the cyber threat environment is considerably worse than it was a few years ago," says **Scott Sayce, Global Head of Cyber at AGCS.** "Therefore, insurers cannot continue in this market without working with clients to provide a strong baseline of acceptable controls that need to be in place."

Cause of loss by value of claims



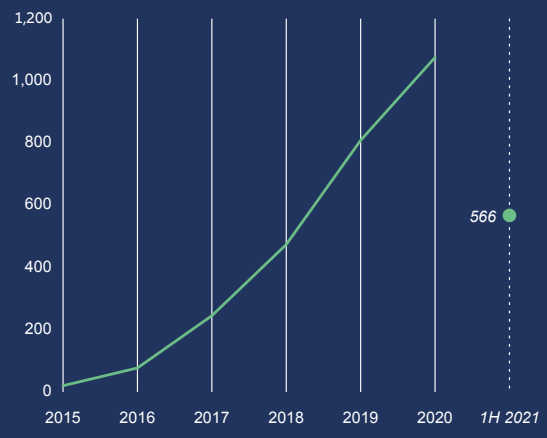
- **External manipulation of systems** — **81%**
  (e.g. direct attack from the internet or malicious content such as ransomware/malware)
- **Malicious internal action** — **10%**
  (e.g. action taken by a rogue employee)
- **Accidental internal cause** — **9%**
  (e.g. human error, technical/systems failure or outage)

Based on the analysis of 2,916 claims worth €751mn (US$885mn) reported from 2015 until June 30 2021. Total refers to all cyber-related claims, not just ransomware incidents. Total value also includes the share of other insurers involved in the claim in addition to AGCS.

Source: Allianz Global Corporate & Specialty

Number of cyber-related claims

per year



*AGCS only started offering cyber insurance in 2013, so claims experience is limited. Total refers to all cyber-related claims, not just ransomware incidents.

Source: Allianz Global Corporate & Specialty


command
option
alt
PASSWORD
1234**

Change is afoot in the insurance market

> Insurers are working with companies to identify cyber security best practices

The ransomware pandemic of the past few years has triggered a major shift in the cyber insurance marketplace, as carriers and insureds endeavor to mitigate the rising frequency and severity of attacks and resulting cyber insurance claims *(see page 13)*.

Cyber insurance rates have been rising (according to broker Marsh[17], US rates rose by over 50% in the second quarter of 2021 alone) while capacity has tightened. Underwriters are placing increasing scrutiny on the cyber security controls that are employed by organizations and pricing risks accordingly.

The role of insurance has always been to encourage good risk management and loss prevention, one that can trace its roots back hundreds of years to protecting the first factories and steam boilers. Although ransomware is still an evolving risk, insurers have been working with companies to identify the best practices and standards that can improve their security postures.

Insurers have established certain cyber underwriting criteria that helps to determine their risk appetite. "Therefore, we are able to clearly communicate our cyber risk management and security expectations. If a commercial customer can fulfil the criteria they will be in a better position when it comes to a ransomware attack and to secure insurance," says Baviskar.

Three out of four companies do not meet AGCS' requirements for cyber security. However, many customers have been working with AGCS to meet the criteria and reduce their exposure. "This approach should encourage companies to invest in cyber security and provide Chief Information Security Officers with ammunition in discussions with their boards," says Baviskar.

17 Marsh, Global Insurance Market Index - 2021 Q2

Good cyber hygiene – risk management pays off

Taking steps to harden cyber security can defend against the majority of ransomware attacks, while robust business continuity and incidence response planning can significantly limit the impact of an incident, should attackers still find a way through.

Analysis of the largest ransomware claims in Europe suggests that the majority of attacks can be avoided. "In around 80% of ransomware incidents losses could have been avoided if the organizations had followed best practices. In many cases we find a lack of multi-factor authentication (for remote access, on privileged IT accounts or for remote maintenance) or inadequate training has been a major contributing factor to the loss," says Daum.

Regular patching and two-factor authentication, as well as information security and awareness training, are essential to avoiding ransomware attacks, as well as just good cyber hygiene. Cyber security tools like endpoint detection and response (EDR) services, and anti-ransomware tool kits and services, can also help prevent attacks, detect threats and accelerate incident response, says Baviskar.

Incidence response and business continuity plans are key to mitigating the impact of a ransomware attack, where planning and a rapid response can make all the difference. Response plans should be regularly tested against ransomware scenarios, while roles, responsibilities and communication lines should be clearly defined. Frequent backups, including those of critical systems and data, are also critical for mitigating the impact and speedup restoration and business continuity.

In the event of a ransomware or other cyber extortion event, companies should follow their incident response plan[18], in particular notifying senior management and the legal department. Looping in legal from the start can reduce the risk of exposure in any class-action lawsuits or other legal claims that may be brought in the wake of the data breach. It is also recommended that the insurance carrier is notified at the outset so that it can determine whether there is coverage under the applicable cyber insurance policy.

Irrespective of the final coverage confirmation, cyber policyholders usually benefit from 24/7 access to emergency incident response services in the first 48/72 hours of a claim. These services typically include a professional crisis manager, IT forensic support and legal advisory. Further offerings include access to online IT security training for employees and assistance with the development of a cyber crisis management plan.

"For many businesses, if they were to improve cyber security, controls and procedures, they would be well protected, and the likelihood of being affected by a ransomware attack would significantly decrease. Hackers will typically hit those businesses with the weakest defenses first," says Daum.

> Hackers will typically hit those businesses with the weakest defenses first

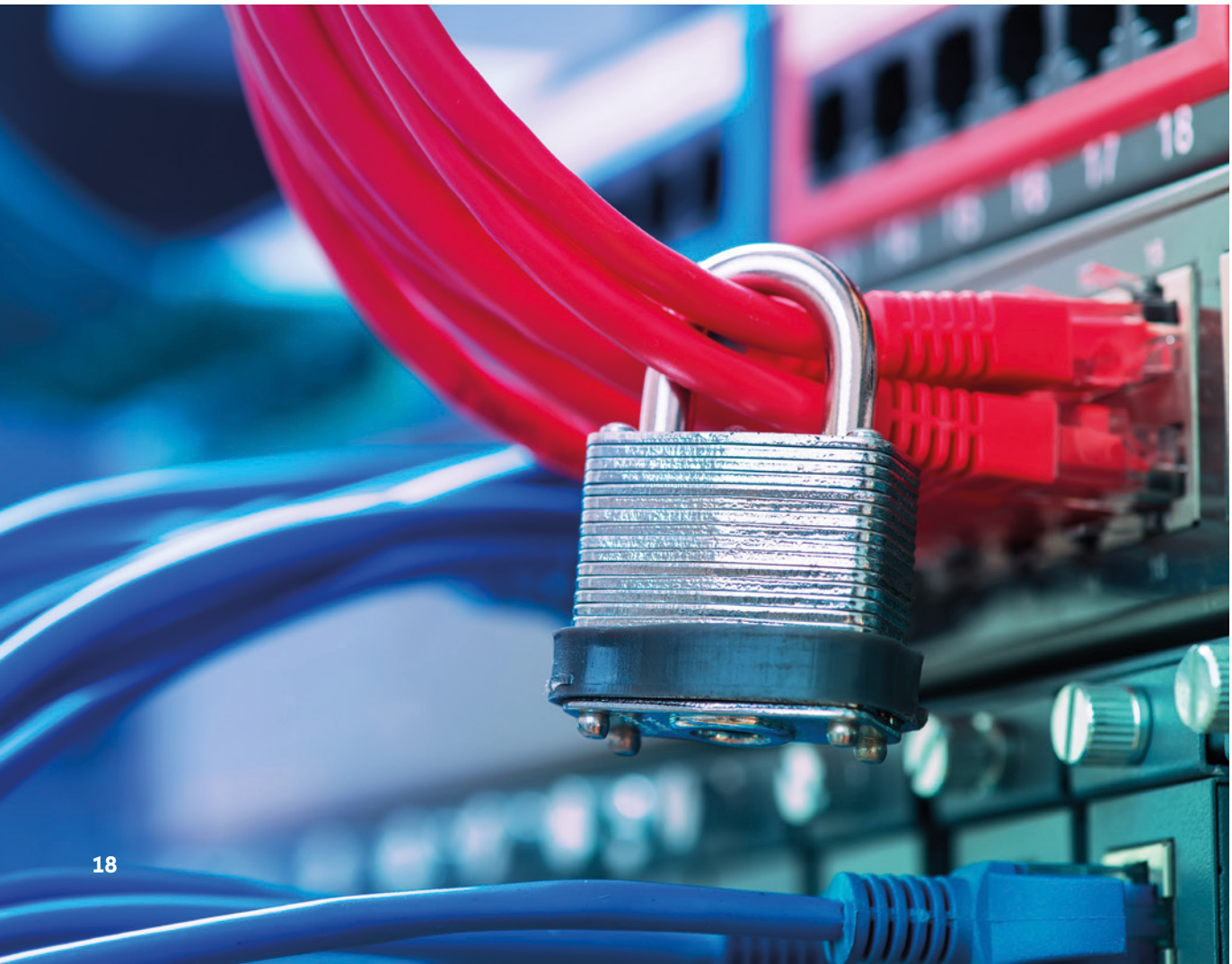
18 Harvard Business Review, Cyberattacks Are Inevitable. Is Your Company Prepared?, March 9, 2021

Creating a sustainable insurance market

If adhered to, best practice recommendations and underwriting criteria should reduce incidents of ransomware attacks, as criminals focus their efforts on organizations with the weakest cyber security and controls. It is also important that companies continuously invest in improving their IT security as there is still a lot of catching up to do. Numerous security gaps can be closed, often with simple measures. By working with clients to reduce the risks of cyber-attacks, insurers can ensure that the cyber market is sustainable for the long run, explains Stanislawski.

"For the majority of companies, ransomware is not going away anytime soon. But for our clients, there is a good chance that this is a problem that can be solved. A house with an open door is much more likely to be burgled than a locked house. We continuously work with our clients to identify and promote the best practices in ransomware protection," says Stanislawski.

Together with the attention that ransomware is getting at a government and company level, there is good reason to be optimistic, says Kang. "Ransomware losses have hit insurers and companies and this activity has given companies impetus to invest in risk mitigation and cyber security. We all have to work together to create a sustainable insurance product."



Ransomware protection – what does good IT security look like?

Ransomware identification:
- Are anti-ransomware toolsets deployed throughout the organization?
- What proactive measures are in place for identification of ransomware threats?
- Are policies, procedures, access controls methods and communication channels updated frequently to address ransomware threats?
- Are in-house capabilities or external arrangements in place to identify ransomware strains?

Business continuity planning/incident response plan:
- Are ransomware-specific incident response processes in place?
- Have there been any previous ransomware incidents? If so, what lessons have been learned?
- Are pre-agreed IT forensic firm or anti-ransomware service provider arrangements in place?

Anti-phishing exercises and user awareness training:
- Is regular user training and awareness conducted on information security, phishing, phone scams and impersonation calls and social engineering attacks?
- Are social engineering or phishing simulation exercises conducted on an ongoing basis?

Backups:
- Are regular backups performed, including frequent backups for critical systems to minimize the impact of the disruption? Are offline back-ups maintained as well?
- Are backups encrypted? Are backups replicated and stored at multiple offsite locations?
- Are processes in place for successful restoration and recovery of key assets within the Recovery Time Objective (RTO)?
- Are backups periodically retrieved compared to the original data to ensure backup integrity?

All of the recommendations are technical advisory in nature from a risk management perspective and may not apply to your specific operations. Please review recommendations carefully and determine how they can best apply to your specific needs prior to implementation. Any queries relating to insurance cover should be made with your local contact in underwriting, agent and/or broker.

Endpoints:
- Are endpoint protection (EPP) products and endpoint detection and response (EDR) solutions utilized across the organization on mobile devices, tablets, laptops, desktops etc.?
- Are Local Administrator Password Solutions (LAPS) implemented on endpoints?

Email, web, office documents security:
- Is Sender Policy Framework strictly enforced?
- Are email gateways configured to look for potentially malicious links and programs?
- Is web content filtering enforced with restricting access to social media platforms?

Segmentation:
- Are physical, logical segregations maintained within the network, including the cloud environment?
- Are micro segmentation and zero trust frameworks in place to reduce the overall attack surface?

Monitoring patching and vulnerability management policies:
- Are automated scans run to detect vulnerabilities? Are third party penetration tests performed on a regular basis?
- Does the organization ensure appropriate access policies, enforcement of multi-factor authentication for critical data access, remote network connections and for privileged user access?
- Is continuous monitoring in place for detecting unusual account behavior, new domain accounts and any account privilege escalations (administrator level), new service additions, and unusual chain of commands being run during a short time period?

Mergers and acquisitions:
- What due diligence and risk management activities are performed prior to M&A?
- Are regular security audits conducted on newly-integrated entities to ensure evaluation of security controls?

Contacts

For more information contact your local Allianz Global Corporate & Specialty Communications team.

Asia Pacific
Wendy Koh
wendy.koh@allianz.com
+65 6395 3796

Central and Eastern Europe
Daniel Aschoff
daniel.aschoff@allianz.com
+49 89 3800 18900

Ibero/LatAm
Camila Corsini
camila.corsini@allianz.com
+55 11 3527 0235

Mediterranean/Africa
Florence Claret
florence.claret@allianz.com
+33 158 858863

Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

North America
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 973 876 3902

UK, Middle East, Nordics
Ailsa Sayers
ailsa.sayers@allianz.com
+44 20 3451 3391

Global
Hugo Kidston
hugo.kidston@allianz.com
+44 203 451 3891

Heidi Polke-Markmann
heidi.polke@allianz.com
+49 89 3800 14303

For more information contact agcs.communication@allianz.com

Follow Allianz Global Corporate & Specialty on

Twitter **@AGCS_Insurance #cyberrisktrends** and

LinkedIn

www.agcs.allianz.com

Allianz Global Corporate & Specialty SE
Dieselstr. 8, 85774 Unterfoehring, Munich, Germany

Images: Adobe Stock

All currencies US$ unless specified

October 2021