GUIDEWIRE

SPECIAL REPORT

2021 Cyber Risk Outlook

What Do the Cyber Trends of 2020 Mean for Insurers in 2021?

- Covid-19 drives increase in ransomware attacks and cyber risk
- 5G to drive up exposure for companies
- US and UK may take regulatory action to battle back against ransomware
- Conditions are ripe for a 'Cyber Hurricane' making landfall in 2021
- Insurers increasingly turn to analytics and modeling to protect against cyber risk

Navigate what's next.

Cyber Risk Outlook 2021: How Evolving Trends Will Impact the Year Ahead

In 2020, the global pandemic created near-perfect conditions for cybercriminals and, unsurprisingly, we have witnessed a sharp spike in cybercrime.

FBI cybercrime reports quadrupled during the first phase of the pandemic; phishing attacks spiked 350%[1] as global lockdowns resulted in more people working from home; and Google continues to block millions of coronavirus-related scam emails each day. Attackers have used increasingly sophisticated and agile tactics to exploit the pandemic by targeting individuals, businesses, hospitals, and schools.

But what is driving these statistics, and what are the implications for cyber insurers as we look ahead to 2021?

2020 Trends: How Criminals Exploited a Crisis

- **Exponential increase in the cyber attack surface**
- **Explosive growth in Ransomware demands**
- **Cyber insurance demand growth alongside climbing loss ratios**

Exponential Increase in the Cyber Attack Surface

The shift to remote work and the large-scale dependency on personal devices and residential networks have expanded threat actors' attack surface — the total number of different points or vectors through which an unauthorized user can try to access or extract data from an environment. Employers are taking precautions, evidenced by the 112% surge in virtual private network (VPN) usage, which allows individuals to securely access their company networks from home, in just the first six weeks of the pandemic.

At the same time, businesses have been digitizing operations at a record pace to adapt to remote working trends, increased virtual consumption, and the need for contactless services. Ninety-three percent of small businesses in a global survey reported more reliance on technology since the start of the pandemic.

The net effect of these changes has been a mass increase in potential targets for criminals to exploit and an unprecedented expansion of company networks beyond their external firewalls. The timing has been fortuitous for criminals: Toward the end of 2019, Guidewire observed a spike in vulnerabilities within gateways and VPNs that have now created ripe conditions for criminals to exploit heightened gateway dependency since the onset of the pandemic.

To say that cyber security under current conditions has proved challenging is an understatement. Businesses were forced to move entire organizations to remote environments rapidly and with little preparation, exposing insufficient IT infrastructures, immature data governance, and inadequate security controls.

Covid-19 triggered an unprecedented expansion in remote working which resulted in a corresponding increase in the 'attack surface' for bad actors. In 2021, the potential targets for criminals to exploit will continue to expand, and corporate networks will be at greater risk.

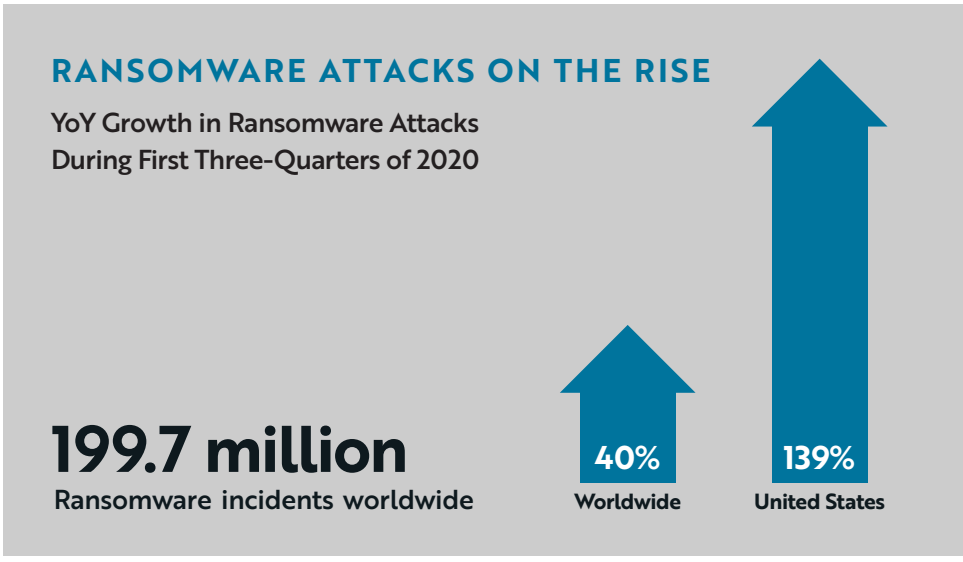
[1] RISKIQ, *Analysis of an Attack Surface: Five Ways Hackers are Targeting Organizations* (n.d., 2020)

Explosive Growth in Ransomware

While ransomware was definitely a problem in 2019, it reached new levels in 2020 with incidents becoming more frequent, targeted, and automated. Global ransomware attacks rose by 40% in the first three quarters of 2020 compared to the same period in 2019, totaling 199.7 million incidents.

The cost of not paying ransoms has also risen. In February 2020, Danish facility services company ISS refused to pay a ransom when criminals encrypted the company's database. Restoring most of the infrastructure and conducting an investigation took nearly a month. Worse, total losses were estimated at $75–$114 million.

Increasingly sophisticated and AI-enabled tactics have seen large business become more and more vulnerable. Criminals have not only accessed companies' core systems; they are successfully infiltrating backup systems as well. An aggressive new tactic has emerged in which criminals extrapolate data from hacked networks and threaten to release it as part of the extortion scheme. Meanwhile, the explosion of "Ransomware as a Service" has lowered the barriers to entry for aspiring cybercriminals, enabling less sophisticated actors to cause significant harm.



Source: SonicWall

Cyber Insurance Demand Grows While Loss Ratios Climb

The spike in cybercrime has driven demand for cyber insurance, and prospective buyers are requesting higher limits. Price and capacity remain notable barriers, however, and it is too early to say if demand will translate into sustained market growth in what is still a relatively new market.

At the same time, underwriting cyber has become more challenging. Three years ago, cyber was a highly profitable line of business with loss ratios as low as 10-15%. Rising claims pushed this figure up to nearly 50% in 2019, and anecdotal evidence suggests cyber loss ratios today hover well above 50%. Some insurers have even reported cyber business loss ratios exceeding 100%. While ransomware is not the only risk at play, it is the primary exposure driving change. According to one major insurer, ransomware accounted for almost 41% of cyber insurance claims in the first half of 2020.

Not surprisingly, the cyber insurance market has turned. Insurers have become increasingly nervous about the deteriorating risk landscape and Guidewire has observed some mainstream insurers withdrawing from the class altogether. Rates are increasing, but a further hardening may be needed to restore confidence.

Despite the challenging landscape, there are reasons for optimism. First, enterprises are more aware of the importance of purchasing cyber coverage. Second, advances in data analytics mean insurers can more accurately price cyber risk and tailor their portfolios to the changing risk landscape. For underwriters equipped with the latest tools in advanced analytics, there is a real opportunity to outperform their peers.

INCREASING LOSS RATIOS ON CYBER

10%-15%
Average loss ratio for cyber insurance in 2018

50%+
Average loss ratio for cyber insurance in 2020

35-40 pt

Source: Guidewire Data

Navigate what's next.

2021 Predictions and What They Mean for Insurers

- **Cyber hygiene will become a differentiator for insurers**
- **Authorities will increasingly intervene as ransomware remains cybercriminals' weapon of choice**
- **Portfolio resilience will take the spotlight**

5G Rollout to Escalate Cyber Risk – Cyber Hygiene Will Be Crucial

Macro conditions will continue to work in favor of cybercriminals in 2021. Even if the global pandemic starts to recede, remote working will persist for some time, and digitization will continue to accelerate.

The rollout of 5G networks will drive the proliferation in connected devices, which already exist in the billions and are largely unmanaged. While 5G will enable a truly digital society, it will lead to security challenges — most notably an even greater number of entry points for attackers to gain unauthorized access, which in turn increases the risk of distributed denial-of-service attacks.

In summary, the expansion of the attack surface in 2021 will increase opportunities for threat actors. The good news is that the anticipated threats are largely knowable and preventable and do not require exotic security measures. In most cases, the cure is relatively basic and mostly center on improving employee awareness and behavior rather than increasing technical capability.

Indeed, businesses that achieve robust cyber hygiene (such as regular patching and password updates) will differentiate themselves from their peers. Similarly, most attacks are initiated by social engineering, and educating employees who are working from home (and are therefore less able to easily verify the legitimacy of email requests with colleagues and IT teams as they would in the office) will reduce susceptibility to phishing and fraud tactics.

For insurers, evaluating cyber insurance customers' use of tools to monitor behavioral indicators of cyber security compliance will be key to achieving excellence in underwriting. For example, the turnover of an IT security team, the patching cadence for software, and the presence of unused services are powerful proxies for whether an organization is fully in control of its cybersecurity. Insurers that can tap into this data via behavioral analytics will have a more sophisticated understanding of risk in their portfolios.

The continued rollout and growth of 5G networks will drive the proliferation of connected devices. While this has benefits in driving a more digitally connected society, it will also lead to greater security challenges—with unlimited entry points for attackers. Now more than ever, businesses need robust 'cyber hygiene' to protect themselves.

Authorities Will Intervene as Ransomware Remains Cybercriminals' Weapon of Choice

The forces driving ransomware are unlikely to change in the short term, for two primary reasons. First, with stolen data sold on the dark web continuing to fall in value, ransoms will remain the most lucrative means of monetizing data breaches.

Second, businesses continue to pay. Many victims believe that paying the ransom is the fastest and most cost-effective option, while criminals know that most large organizations have insurance that not only covers ransom demands but also supports payment in cryptocurrencies. These factors are only serving to fuel the growth in this crime and the size of ransom demands.

As ransoms continue to grow, regulators and government authorities will be forced to intervene either in the payment of ransoms, or the use of cryptocurrencies, to slow the vicious cycle. So long as the economic and reputational costs of not paying outweigh the price of the ransom, this will be a Herculean challenge. But there is a growing consensus that something needs to be done to reduce the growth of ransomware.

In the UK, the former head of the National Cyber Security Council (NCSC), Ciaran Martin, has called for "urgent" action that includes a change in law to prevent businesses from paying ransoms and to make ransomware risks a board-level problem. In the US, the government is tightening its grip, issuing guidance in October reiterating its position that cyber insurers that make ransom payments to certain threat actors to be in violation of the law.

Insurers must watch these trends closely. Experience in the kidnap and ransom market tells us that if governments succeed in making ransoms harder to collect, criminals will shift their tactics to achieve payment via alternative channels. Demand for indemnification will continue to exist, but insurers must actively monitor changes to criminals' modus operandi and continuously assess the relevance of their cyber insurance products.

WATCH FOR REGULATORY CHANGES AS RANSOMWARE PAYOUTS SOAR

$500,000 Average ransomware payment

2x So far this year

Source: Guidewire Data

Navigate what's next.

With Potential for 'Cyber Hurricane' Event in 2021, Portfolio Resilience Will Take the Spotlight

In 2021, the focus will turn to portfolio resilience as insurers and regulators take a growing interest in the scale of cyber accumulation risk and its impact on capital—this will drive demand for cyber insurance.

There has yet to be a cyberattack large enough to become a rating event, but the potential is there. Models run by Lloyd's and Guidewire indicate that a single cyber event such as a major cloud service provider hack could cause losses as large as a major hurricane — with the potential to increase industry loss ratios anywhere between 19% and 250%.

For insurers to expand capacity to meet demand, they will need to think more carefully about potential balance sheet impacts from a catastrophe-scale event. The technical pricing of individual policies will remain important but understanding the potential for aggregated losses is now vital; in particular, it demands closer cooperation between underwriting and capital management teams.

We expect focus to turn to accumulation tools to deepen the industry's understanding of portfolio dependencies. Cyber accumulation risk indicators exist but are generally less tangible and less understood than for traditional risks. Examples include a dependence on a common service provider or using the same version of a particular type of software.

This coming year may see the market's first major 'Cyber Hurricane.' Models run by Guidewire indicate that a single cyber event, such as a major cloud service provider hack, could cause losses as large as a major hurricane. We expect insurers will put an increased focus on portfolio resilience to counter this threat.

THIRD-PARTY RISK AGGREGATION MANAGEMENT NOW KEY FOR GROWING NUMBER OF INSURERS

40% Percentage of insurers using using external vendors to help manage aggregation in 2020

16% Percentage of insurers using using external vendors to help manage aggregation in 2018

94% Percentage of insurers using third-party vendors to identify top risk factors and expected loss estimation

Source: 2020 survey from Advisen Ltd

[2] Partner Re and Advisen, *Cyber Insurance – The Market View* (Sept. 17, 2020)

GUIDEWIRE

Summary: Technology Is a Human Risk

Like all criminals, cybercriminals are driven by three things: motive, means, and opportunity. Their motive and means have certainly not diminished in 2020, and their opportunity has expanded substantially.

The above themes are propelled by two underlying dynamics. The first is obvious: We live in a world that is increasingly reliant on technology. Second, the way in which the technology is deployed is driven by human factors (an argument explored in more detail in the Guidewire blog post, Why Insurers Should View Cyber as a Human Risk, Not an IT Risk). Guidewire's analysis of the causes behind recent cyber claims has demonstrated that behavioral factors are valuable tools for predicting future cyberattacks, as well as for understanding cybercriminal tactics.

Insurers must ensure they have the appropriate tools to understand cyber risks in this tech-enabled world, and behavioral analytics will become a vital weapon in their arsenal. Ransomware has been the cybercrime story of 2020, but understanding the human drivers behind it will be key to unlocking our understanding – and ability to successfully insure – this risk.

Document Published: 2020-12-9

Navigate what's next.