**Ransomware Has Been a ‘Game Changer’ for Cyber Insurance**

By [Elizabeth Blosfield](https://www.insurancejournal.com/author/elizabeth-blosfield/) | August 30, 2021



Anyone who works in cyber insurance knows that the industry is never static. It’s a constantly evolving business as the risks change all the time, and this has never been more apparent than right now, said panelists for Insurance Journal’s recent webinar – [Cyber Insurance: Is This the Beginning, Middle or End?](https://www.insurancejournal.com/research/research/cyber-insurance-is-this-the-beginning-middle-or-end/)

“The game changer,” said Justin Herring, executive deputy superintendent at the New York State Department of Financial Services (DFS), “has been ransomware.”

Ransomware attacks accounted for nearly one quarter of all cyber incidents globally last year, according to software company Bitdefender.

“I always think of December 2019 as the tipping point for when we started to see ransomware take hold,” said Bob Wice, global head of underwriting management for Cyber & Tech at Beazley.

Indeed, the U.S. was hit by a barrage of ransomware attacks in 2019 that impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion, Emsisoft reported on its blog.

“And you just see with each passing year, but sometimes it seems like almost with each passing month, we’re seeing more and more of these events,” Herring said.

A spate of recent attacks this year have been of particular concern among U.S. government officials, as they’ve been [attributed to cybercriminals operating from Russia](https://www.insurancejournal.com/news/national/2021/07/08/621751.htm), Insurance Journal [previously reported](https://www.insurancejournal.com/news/2021/07/14/622254.htm). There was the hack last year in which Russian military cyber criminals sabotaged computer code [within a software called SolarWinds](https://www.insurancejournal.com/news/national/2021/02/16/601294.htm). Now, a July ransomware attack has made its way to the center of the conversation, in which [the Florida information technology firm Kaseya](https://www.insurancejournal.com/news/national/2021/07/06/621412.htm) saw its management system hacked. REvil, a Russia-linked cybercrime syndicate, took credit for the breach.

In June, REvil [extorted an $11 million ransom out of meatpacker JBS](https://www.insurancejournal.com/news/national/2021/06/10/618052.htm) after compromising its supply chain. Earlier this year, in May, an intrusion by another Russia-linked group at [U.S. fuel transporter Colonial Pipeline](https://www.insurancejournal.tv/videos/19374/) led to the shutdown of 5,500 miles of critical infrastructure, causing panic buying and gas shortages all along the East coast.



“You can also see that we’ve had cyberattacks recently where an attack that went through a widely used technology gave access to or disrupted or potentially disrupted many organizations,” Herring said. “Similar types of attacks against IT or technology vendors or service providers have disrupted in one shot half a dozen, a dozen or more of DFS’ regulated companies.”

Herring said that a growing interdependence on technology, particularly during the ongoing COVID-19 pandemic, has made companies and organizations more vulnerable to the type of cyberattack that can have systemic effects.

“[We’re seeing] attacks effectively on our technology that we are growing more and more dependent on,” he said. “Attacks against a single institution or a single organization where there’s a disruption there, and that disrupts a lot of downstream organizations.”

Wice agreed, adding that businesses and individuals alike have been more at risk of [cyber incidents involving social engineering](https://www.insurancejournal.com/magazines/mag-features/2021/05/17/613684.htm), or cyber crime that capitalizes on human error, than ever before.

“During the pandemic, a lot of this was about remote access, ports being opened and phishing,” he said. “People [could be] looking at a map that was sent to them about where the cases and death rates were in certain jurisdictions, and lo and behold, there’s a bad link in there. And so that’s how a lot of these attacks were happening from March 2020 onward.”

**Moving Towards Education**

On a positive note, said Marc Voses, partner at Clyde & Co., all of this has led to greater public awareness around cyber incidents, with more companies trying to harden their cybersecurity posture.

“Not a day goes by when we don’t see an article or see a newscast which basically says companies need to get their houses in order with respect to cybersecurity,” he said.

And companies largely are listening, Sylvestro agreed.

“I think we’re reacting by going towards education, and I think that’s a really good thing,” he said. “And I just hope that we continue to do that because cyber risk is not going away. We’re not going to be moving away from using computers, from using email, from processing data.”

Sylvestro said the best way insureds can make sure their coverages are as robust as possible is to closely examine the exposures insurers are telling them to reduce.

“Insurers don’t tell us to do those things just so we have another thing to add to our checklist,” he said. “They do it because they don’t want to have to deal with a loss and our clients don’t want to have to deal with a loss.”

Without good cyber hygiene, insureds “will find themselves at the mercy of the market,” he added. “And I can tell you from experience, that’s not a fun place to find yourself.”

Herring added that it’s important for insureds to take steps like using secure passwords, securing any poorly configured ports or machines within their network, patching vulnerabilities and using a minimum number of privileged accounts to manage their network.

“I think the good news is that it is possible to prevent most ransomware attacks, or at least for organizations to significantly reduce their risk of suffering a ransomware attack,” he said. “And if they do suffer a ransomware attack, there’s an opportunity to significantly reduce its impact either through catching the attack earlier in the process or through things like having good backups from which the company can recover.”

**More Questions Than Ever**

For insurance agents, on the other hand, the challenges around cyber coverage are equally as critical.

“It is complex. It is complicated. It’s difficult to understand,” Sylvestro said. “There are more questions now than there ever have been.”

Because of this, he said it is important that brokerages and agencies are investing in education and understanding what cyber risk truly is.

“I would just encourage everybody in the industry to take some time to really invest in your education, to invest in finding new ways to learn more about this space, whether it’s reaching out to insurers,” he said. “A lot of insurers are providing a lot of education around cyber risk, and they’re happy to share that because they see a vested interest in it as well.”

Voses added that cyber insurers can shield their own risks in this area by updating policies if needed with language that reflects current exposures. This can help avoid challenges where insureds are without coverage in a needed area or where silent coverage is being provided under a cyber policy that wasn’t intended by the insurer.

“Many of these policies have been in the market for years now,” he said. “Some of them have not been subject to a refresh or a review of the coverages being provided.”

Additionally, addressing the scope of coverage and including relevant exclusions or sub-limits can be important as part of a policy refresh, Voses said.

“I think it can be easy to feel like you’re trying to fill a cup of water at the bottom of Niagara Falls in this space right now,” Sylvestro added. “And the better equipped we are as brokers, the more symbiotic our relationship is going to be in placing risk.”

Wice said that for underwriters, it’s just as important to react to losses as it is to attempt to avoid them in the first place.

“It’s focusing in on trying to understand where the losses are and yes, it is somewhat reactive, but that is the golden goose to try to figure out what the next threat is going to be,” he said.

**Not an Insurmountable Risk**

While Herring said DFS has taken the view that cyber is currently “the biggest risk for the financial services industry at large,” it’s not necessarily an insurmountable problem for insurers, especially the big players in the industry.

“But it is a challenging problem because this is an area where change happens rapidly,” he said.

The best thing both insurers and insureds can do is stay vigilant, he explained.

“One of the things that I encounter is what I think of as a sense of cyber fatalism,” he said. “If you’re not a professional working in this field every day, you probably learn a lot of what you know about cyber from major news events.”

Herring said this can lead to a skewed perspective in which cyber risks feel like an impossible mountain to climb.

“For every Solarwinds type attack…there are 99 other cyberattacks, the vast majority of which are using well understood and tried and true hacking methods,” he said.

In fact, in its analysis of cyber incidents affecting DFS-regulated entities just this year, Herring said the regulator discovered many hackers are using the same basic playbook, with the number one attack method being phishing in which email is typically used to solicit personal information by pretending to come from a trustworthy sender.

“I think what we hope people will take away from that is that despite what you read in the news, you actually can reduce this risk,” he said. “You can protect yourself from most of the attacks that most organizations are facing most of the time.”

However, that doesn’t mean insurers and their clients can get comfortable with cyber risk just yet, Sylvestro warned.

“I think every time we feel like we have some kind of handle on it, or we’ve got some real compensating controls, threat actors continue to invest in their craft as well,” he said. “So I think it’s important to understand that when we talk about ransomware, we’re not talking about this static type of threat. It’s something that grows and evolves and shifts, and we have to continue to be vigilant as we deal with that as an industry. Otherwise, we could easily find ourselves well behind the eight ball even more so than we are now.”