Insurance POST

Q&A: Erin Kenneally, Guidewire

Harry Curtis

11 Aug 2021

Indicative reading time: 5 minutes

Erin Kenneally, director of cyber risk analytics at Guidewire, discusses the changing face of cybercrime, how cyber insurers can improve, the case for prohibiting ransom payments and the looming threat of supply chain cyberattacks.

How did you become involved with cybersecurity?

I've been involved at the crossroads of technology, law and policy for pretty much my whole career. By training I'm actually an attorney and I started working at the San Diego Supercomputer Center out of law school.

I've had various roles in industry, government and academia. Before joining Guidewire, I was at the US Department of Homeland Security, where I worked in the cybersecurity division. I've always been attracted to and driven by solving hard, systemic problems, and cyber risk is definitely a poster child in that regard.

Ransomware has been on the rise in recent years. Why is this happening?

Statistics vary and they're never really comparing apples to apples, because everyone sees different parts of the elephant. But what all the statistics agree on is that the frequency and the severity of ransomware is on the uptick for sure.

When you look why ransomware has been so successful and continues to be successful, it's a matter of behavioural economics in my mind. Ransomware enjoys higher reward for less effort and lower risk. It's a perfect storm.

There's no shortage of vulnerable systems, and that's been **exacerbated by Covid-19**. The migration to working from home has blown up the attack surface and amplified the traditional attack paths, like open [remote desktop protocol] ports, vulnerability exploits and phishing.

Then there's definitely a lower barrier to entry for bad actors to get into the ransomware game. The code is available in more formats. It impacts more platforms. It's available in this ransomware-as-a-service modality. The technical sophistication to execute a ransomware attack is pretty low.

There are also high profit margins for the bad actors. The year-on-year the average ransom paid increased 173%. In 2019, the highest extortion paid was $5m (£3.6m). We saw CNA pay $40m this year. That's huge.

Finally, there are low transaction costs. Bad guys can leverage cryptocurrency as a way to achieve direct payouts and monetise their denial of access more directly. They used to have to abscond with data, launder it and sell it through the dark market, which is fraught with uncertainty, transaction costs and latency whereas ransomware allows them to get their bounty immediately.

Can you explain what double and triple extortion tactics are?

Double extortion is where bad actors will basically exfiltrate the data before they either lock the system or they encrypt the data. Frankly, it's become the norm. For example, the police department in Washington DC recently got hit, and after negotiations broke down, the attackers threatened to post psychological evaluation reports of police officers and informants.

Triple extortion, which is the newest technique, is where, instead of targeting a single, large-scale company with one large-scale ransom demand, there are also accompanying individual ransoms for affected parties. A good example is a Finnish psychotherapy firm, which was locked down, and had the records of around 40,000 patients exfiltrated. Some of those 40,000 were also sent extortion notes asking for 200 Bitcoin, which is a lot more than $200.

How important a role does cyber insurance play in protecting businesses?

We can't reduce the risk to zero, even for the best protected companies and cyber insurance is the critical way to transfer that risk. Frankly, it's a critical infrastructure in and of itself. Right now, the cyber insurance market is becoming a hard market. Less is being underwritten, and the downside of that, in the face of this onslaught of ransomware attacks, is it's really underserving the need on the ground to transfer the risk. The bottom line is that there's **definitely a need for an insurance solution** for this for this risk.

How can cyber insurers improve?

Traditionally, the approach for insurance companies in the face high loss ratios is to resort to conventional **pricing levers**: increased premiums, increased deductibles, lower limits, cut the scope of coverage. Taking that approach in the face of this peril is not the path out of the problem. It's a one-dimensional approach to a multi-dimensional problem.

So what can they do? Number one is embracing their role as incentivising information security, loss prevention, and mitigation controls. We see some of the top carriers and even some of the lesser carriers embracing this role. Things like refusing to bind or renew a company if it can't attest to having certain security controls in place, incentivising and instituting things like premium reductions for those that have a clean bill of cybersecurity health, as it were. There have also been suggestions of changing the policy cycle in order to be more agile and responsive to cyber exposures because cyber exposures don't operate on the annual timeframe that policies do.

Second, there also needs to be more active coordination between underwriters and insurers and the information security professionals at the insured company. It's one thing to incentivise controls, but you also need metrics because the risk is dynamic.

Third, cyber insurers need better descriptive and predictive models, which requires having more and better incident data. Read any report on the state of cyber insurance, and you will hear laments over the lack of actuarial data to give confidence in underwriting. Insurers can improve that by sharing claims data in the proper manner and also by doing a better job of controls failure reporting. There's a huge disconnect between the front-end assessment of the risk, the guidance that's shared between the underwriter and a company and the back-end claims data collection. Often, the source and causality of the cyber event is left on the cutting room floor and it's not used to inform the front end. Significant progress can be made by collecting that data.

Finally, I would just advocate for consensus, consistency, and leadership with regards to policies against ransom non-payment. We've heard a whole bunch of news in that regard with no real progress. Axa XL took the stance that it won't write extortion payments. Beazley came out and said the opposite, and said denying extortion payments is a job for the government. It's an area where there's definitely **strong sentiment** that by paying the extortions, the industry has actually encouraged the growth of ransomware.

Is there a case for banning insurers paying for ransoms?

A policy prohibiting payments would do more good than harm. You've got to be concerned about situations where if you prohibit payments, then the parties that are in the weakest position to protect themselves will be harmed the most, so there should be exceptions made. For instance, in healthcare situations, prohibiting a hospital from paying a ransom across the board isn't helpful, especially if you've got life and limb on the line.

The US Secretary of Homeland Security has put forward the idea of working with industry to create some sort of a fund so that if there is a prohibition, there's a fund that can be pulled from to stem the tide for companies.

The ultimate backstop though is for companies to harden their infrastructure and to increase their information security controls. Just to continue to pay and leave your systems exposed just invites the bad actors to continue to do this. Banning it and having a period of time where we provide support for companies in order to get up to speed with their with their information security controls is probably the path forward.

What other government actions would be helpful?

One thing [the US] government can do is ransomware disclosure regulation. If you think about the one area where the cyber insurance industry has pretty strong footing from the standpoint of actuarial data, it's data breach. Why is that? It's on the back of state data breach regulation that the industry was able to build up actuarial data and have the confidence to underwrite these risks.

Ransomware – with the exception of the healthcare industry because healthcare deems a ransomware event to be a data breach that requires disclosure – does not require reporting. We've got all these blind spots that we don't know about. If the government were to require reporting of ransomware events, that would be a huge step forward.

Does the recent surge in ransomware attacks represent the high-water mark for cybercrime or is there worse yet to come?

I'm always hesitant to say that we've seen the worst. I don't believe we have. We're definitely going to see more supply chain-related attacks, which will cascade into systemic harms and losses, though I certainly don't wish that.

Most recently we've seen the Kaseya attack on the [IT managed service provider] supply chain. It's about where bad actors can get the most bang for their buck. Right? Do you attack an MSP and then get access to hundreds of thousands of their customers, or do you individually go after each customer? It's a no brainer there. That's the trajectory they're headed down, and our ability to understand the cyber supply chain and the cascading effects of attacks on the cyber supply chain is quite challenged right now. That's where we have significant vulnerabilities moving forward.

MARK AS READ