Illuminating the dark world of ransomware

Although cybersecurity has been gaining prominence in the collective consciousness for some time, it received an unprecedented degree of attention earlier in 2021.

This year began with the SolaMinds hack ringing in the world's ears-and the drumbeat of notable cyberattacks has continued ever since.

As 2021 has unfolded, though, ransomware, more than espionage, has been the word on everybody's lips. This type of malware encrypts user data and blocks access until payment of a ransom, and it has been around for decades. In the last few years, though, it's been escalating.

The rise of ransomware is startling. AIG has predicted that ransomware could cost $20 billion in 2021, up from $315,000 six years before. No longer involving just locking the files of unfortunate individuals who wandered onto the wrong website, ransomware has grown into a sophisticated business that can disable huge corporations for days at a time.

In May 2021, attacks underscored the vulnerability of critical infrastructure by causing fuel shortages in areas on the United States' East Coast served by the Colonial pipeline, disruption to the Irish health service, and shutdowns for meat processing giant JBS from Canada to Australia. This triumvirate of attacks bolstered the argument that ransomware has transitioned from a minor commercial menace into a national security threat.

Perhaps the growth of this particular form of cyberpiracy shouldn't come as a surprise after cybersecurity firms reported an increase in cases of between 150 per cent and 485 per cent during 2020. Nonetheless, many companies are clearly unprepared for the wave of attacks crashing over us.

An argument exists that external factors have caught some unawares: Millions of employees suddenly accessing commercial data from home systems presents an almost unavoidable weakness. The human psychology associated with the C0VID-19 crisis probably contributed, too, with fear, distraction, and novelty making it more difficult to discern which communications are legitimate and which aren't and turning the pandemic into a phishing paradise..

However, many attacks continue to exploit issues that could have been prevented by either the company or employees, as seen with Colonial's admission that a single disused account was compromised in its case.4 Multifactor authentication and better cyber-hygiene awareness won't suddenly make companies hack-proof, but they will certainly help.

The proliferation of attacks is supported by increasingly sophisticated business models used among hackers. DarkSide, the ransomware group that became a household name after the Colonial attack, operated a profit-sharing model with a suite of services offered to would-be hackers alongside terms and conditions. In addition, adoption of a model similar to the McMafia criminal franchise is growing in ransomware circles.

The increasing inclusion of user-friendly interfaces and customer service in ransomware-as-a-service (RaaS) packages lowers the barriers to entry for less technically sophisticated franchisees.

Perhaps inexperience and complacency have an upside: In an unusual outcome, the FBI was able to recover a large chunk of the Colonial ransom after acquiring the private key to the hackers' Bitcoin willet. Yet the influx of so many attackers is a troubling development – and one that presents a quandary for governments, businesses, and the insurance industry.

To Pay or Not to Pay

At the heart of the multifaceted dilemma facing government and business victims is whether to pay a ransom.

The downsides of doing so are obvious and numerous. Primary among them is the glaring truth that making a ransom payment supports and encourages cybercrime. Hackers and other cybercriminals become increasingly motivated and, in a world of unfettered capitalism, smart ones go away and invest in product research and development, marketing, and customer support architecture to make their attacks better and their product easier to franchise.

The U.S. and U.K. governments both advise against paying ransoms, further noting that companies have no guarantee of getting their data back. Statistics back up this stance: According to cybersecurity companies Kaspersky and Sophos, only 29 per cent of people who paid the ransom recovered all their files, and just 8 per cent got all their data back.

Some analysts have posited that increasingly inexperienced hackers using off-the-shelf tools may not even know how to decrypt the systems they've locked down – yet knowing that doesn't necessarily make it easier to decide what to do when ransomware strikes.

With data suddenly in the hands of a hostile actor and a strong business imperative to avoid revealing a leak that might cause severe reputational damage, many companies choose to pay. There are many estimates of the exact percentage of victims who pay the ransom, but any figures are prone to wide margins of error, as those who pay quickly are disincentivised to report a breach to markets or authorities.

This raises the other side of the dilemma: While governments may not like it, paying the ransom can make business sense, at least in the short run. Insurers and businesses know that paying the fee is likely to be less damaging and expensive than the cost of treating the attack as a hardware issue and starting from scratch, improving security architecture as part of a rebuild.

With data locked and operations in disarray, the prospect of the commercial cost racking up is typically motivating enough. More often, however, cutting-edge malware entrepreneurs have realised the implications of peeling off and threatening to expose sensitive data or selling it on the dark web.

These "double-extortion" attacks force companies to also deal with the prospect of reputational damage that can generate unquantifiable costs on top of disrupting day-to-day business. Leaked personal client data can repel customers and attract attention from regulators. In this context, paying for a quick resolution seems understandable – a solid, quantifiable charge to get things back to normal against as-yet-unknown expenses that mount as the hours tick by.

When an organisation chooses to go down the no-negotiations route, things can get very expensive quickly. Famously, the city of Atlanta decided to rebuild from scratch rather than pay a $51,000 ransom to unlock municipal computers, at a cost estimated at $17 million.

For some companies, the cost of the ransom plus the cost of a shutdown can threaten their very existence. In anticipation of such circumstances, transferring the risk of covering the ransom to an insurer seems to be a logical and reasonable solution. Then again, systems are always going to need upgrading. If weaknesses aren't identified and resolved, hackers will simply reinfect the system-as some unfortunate companies have learned – generating significant costs.

The Effects of Geopolitics on Cybercrime

States generally lack the regulation to deal with this new threat. Plus, while governments may find paying ransoms distasteful, any attempt to outlaw it will likely chase the practice further underground. Moreover, it criminalises the victim, who may end up garnering public support under term inning that the consequences of not complying with the law are worthwhile- if a $1 million ransom attract a $100,000 fine, that represents less of a deterrent then it does a 10 percent tax on data recovery.

This dilemma is arguably trickier than the one companies face on the receiving end of a ransomware attack. Still, it's leading to governments' staying on the sidelines and batting the dilemma to the commercial space. The politics of a ban on ransom payments will remain fraught as long as the problem is growing. If the expansion can be brought under control, it'll become easier to deal with the relatively fewer cases move careless or unfortunate businesses that suffer an attack.

A more predictable environment would also help to model the phenomenon. So why, if ransomware damage costs so much, are we not able to effectively police it? Answering that question requires stepping up a level again, to geopolitics.

International affairs become crucial because few cybercriminals are based in the West. FBI Director Christopher Wray has specifically singled out Russia, and a list of the top earners from ransomware is a who's who of the Russian cyber underground.

The targets, however, are mostly in the West. While that can be partially attributed to some of the largest companies being located there, ample evidence suggests that the criminal groups intentionally seek to avoid targets in Russian-speaking areas.

The groups enjoy the benign neglect of local security services by acting as a thorn in the side of geopolitical rivals and being careful not to upset anyone closer to home. Again, nothing is new here; tolerating outlaws who annoy your enemies is a phenomenon older than the modern nation-state.

With Russia joined by countries such as China, North Korea, and Iran in refusing to cooperate with western law enforcement, attackers are operating in a high-reward, low-risk environment that pays enormous dividends for skilled ransomware writers.

The problem has finally grown large enough to enter the geopolitical sphere in its own right, especially given recent attacks on major infrastructure. Hackers seem to be aware of this fact; DarkSide issued an apology for the colonial disruption and implied that a RaaS customer has been responsible for the inappropriate target selection.

Still, this level of disruption to infrastructure would constitute a major attack if conducted by the government using bombs or sabotage, The U.S. has made clear that it's willing to respond with its own disruptive measures. As of this writing, the effect of this threat remains uncertain. But simple economics suggests that unless countries cooperate to make it too risky to pursue expected payouts, the entrepreneurial will continue to gravitate towards cybercrime.

The Central Role of Insurance

Being asked to step into a legal void on the morality of paying ransoms is probably beyond the remit of insurers, whose domain is risk transfer, not political philosophy. Still, as a recent paper by the Carnegie Endowment notes, insurance can facilitate change by incentivising better management and cyber hygiene. Some argue that cyber insurance incentivises poor security practice, which is similar to saying that homeowners insurance encourages leaving the door unlocked. It is, perhaps, simply indicative of a young market that hasn't found the proper policy wording and pricing to mitigate the inherent moral hazard. We must be hopeful that this will change.

It might be cheaper to pay a ransom than rebuild a system from scratch, but training for staff and basic cybersecurity procedures could be less expensive than both. Insurance pricing and policy terms should act as additional incentives for spooked companies.

A Deloitte report suggests that insurers could benefit from applying more robust scrutiny to cyber insurance applicants to align more closely with major commercial property insurance products. As the market tightens and prices rise, scrutiny is sharply increasing, a correction that may well be positive. As criminals get greedier, insurers may reconsider the cost-benefit analysis of paying ransoms, a trend that could eventually be fatal to the practice of ransomware attacks.

It's unlikely that the problem will ever be resolved without progress within and among states regarding approaching the root causes of cybercrime. International cooperation won't instantly weed out all state-endorsed cybercrime either, any more than international law stopped all wars. Yet it could develop into a broad understanding of what is and isn't acceptable.

In the meantime, cooperation between governments and industry to improve incentives for firms to upgrade their security architecture is likely key to bringing cyber risk back under control.

Governments are critically positioned to facilitate information sharing and to legislate, cajole, and subsidise businesses in the direction of improved cybersecurity. They should also provide clear legislation and guidelines on what they expect insurers and other companies to do to help with this task.

Insurers should continue to work with the government to increase risk awareness and bridge the data gap, sharing information and finding ways to encourage cyberattack reporting that will help the sector price risk better. But they can't tackle the problem alone. As the American Property Casualty Insurance Association (APCIA) 's new ransomware guiding principles point out, insurance is only one aspect of national cyber resiliency.

Ransomware has developed in the space created by geopolitical standoffs and thrived amid the unique circumstances of the C0VID-19 pandemic. It is a societal malaise that will require a societal effort to control.

Governments are the only entities that can pursue and disrupt ransomware groups, are critically positioned to coordinate between parties, and are responsible for creating a clear operating environment for companies. Yet, as cyber threats become more complex, insurance remains an essential part of the resilience and risk management framework.

Daniel Ridler - Head of Information Risk and Data

This article was originally published in the fall edition 2021 issue of Insights: A Professional Journal by the CPCU Society and is shared with permission from The Institutes CPCU Society. All rights reserved. www.CPCUSociety.org.