Too Big to Fail: Recent Cybersecurity Incidents Highlight Critical Infrastructure Vulnerabilities

July 26, 2021

CONTACT

HALIFAX

Matt Saunders, CIPP/C
(902) 491-4221
msaunders@coxandpalmer.com

HALIFAX

Peter Faour
(902) 491-4457
pfaour@coxandpalmer.com

As the COVID-19 pandemic and its fallout continues to challenge health care systems, supply chains, and essential services around the world, the growing cybersecurity threat of ransomware must be addressed by policy makers given its potential impact on already strained critical infrastructure networks.

What is ransomware?

Ransomware is a type of extortion software that can lock your computer, encrypt your files, and then demand a ransom for their release. Generally speaking, it is a type of malware (i.e., software that is malicious) that can impact an entire networked computer system or just a few files on a single machine.

In the early days of ransomware, hackers would deploy malicious software on unsuspecting businesses and then impersonate response teams to unlock the affected systems. Ironically, the hackers would be paid for the problem they created while also being acknowledged as having remedied the situation.

Ransom became hackers' go-to method of payment with the arrival of Bitcoin in 2009, however. From that point on, the ransomware market has evolved significantly. For example, developers now sell malicious programs to individuals looking for a payday in exchange for a percentage of the ransom paid for an attack (even though they had no part in the operation). With the commodification of the market, the average ransom payment in 2021 rose to $220,000.

The Ever-Growing Risk

The impacts of ransomware are not just financial. Christopher Ray, the Director of the Federal Bureau of Investigation, recently testified that the challenge raised by ransomware for the United States is similar to that of the 9/11 terrorist attacks, and warrants a comparable (and coordinated) response. There have been no shortage of incidents grabbing headlines – particularly over the course of the pandemic – where ransomware has seriously impacted or fully shutdown critical infrastructure assets around the world.

HEALTHCARE

In September 2020, a woman in Germany became the first known person to die as a result of a cyberattack. The woman was turned away from a hospital in Düsseldorf after the facility fell victim to a ransomware attack that encrypted its servers. The patient was then diverted to the next nearest hospital, over 30 kilometers away, for her operation. Sadly, the woman died en route as a result of the delay in patient care caused by the cyberattack.

UTILITIES

In February 2021, the city of Oldsmar, Florida narrowly escaped disaster when an operator at a city water treatment plant noticed his computer mouse moving across his screen on its own. His device then attempted to make a system change that would have released large amounts of lye into the

town's water supply. Luckily, the operator acted quickly and was able to prevent the release. The subsequent investigation determined that a hacker had remotely seized control of the water utility's computer and attempted to poison the town's water supply. The hacker's motives and identity remain unknown.

ENERGY

In May 2021, cybersecurity was in the headlines again after gas prices surged and shortages loomed along the eastern seaboard of the United States. The Colonial Pipeline, responsible for delivering approximately 45% of all fuel consumed on the East Coast, suffered a ransomware attack. Colonial proactively shut down the pipeline in response to the incident and ultimately paid a $4.4 million ransom to the attackers. The FBI later confirmed that the DarkSide ransomware was employed to attack Colonial, likely by criminal group operating out of Russia. In an interesting twist, the FBI has since been able to recover $2.3 million of the ransom by tracking the ransom payment, made in bitcoin, as it was transferred through several digital wallets.

FOOD SUPPLY CHAINS

In another recent ransomware attack, the world's largest meatpacker, JBS, was forced to shutter operations in Australia, Canada, and the United States for several days. Early indications suggest that, similar to the Colonial Pipeline attack, the responsible party is a criminal organization operating from Russia.

INTERNET ECOSYSTEM

Earlier in July, the Russian-speaking digital gang, REvil, targeted Kaseya, a managed services provider (MSP). Through a "zero day" attack – where hackers exploit a previously unknown flaw in a system – REvil was able to use its virtual system/server administrator platform to encrypt servers and workstations around the world. Put simply, Kaseya's thousands of small and medium-sized business clients became virtual dominoes in the ransomware incident: by targeting a critical point in the Internet ecosystem, REvil was able to turn a single attack into one of the biggest hacks in history. In Sweden, for example, one of the country's largest grocery store chains had to shutter its 800 locations for days as the ransomware attack had crippled their cash register system.

These recent ransomware incidents highlight that no organization or industry is safe from cybersecurity threats. Not only are these types of attacks incredibly damaging to the reputations and bottom lines of the companies affected, but these cyber incidents are increasingly threatening to the lives of those who rely on such critical infrastructure systems.

Data Privacy Implications

These health and safety, financial, and reputation risks are compounded by the data security issues arising for critical infrastructure organizations that handle personal information. Business leaders cannot lose sight of the potential statutory requirements and penalties for organizations who collect personal information (and fail to protect it). Look no further than the risk of ransomware 2.0 attacks where data is exfiltrated and copied before it is encrypted. This step allows cybercriminals to extort the victim even if they have back-ups of the impacted systems/information. If the victim fails to pay, the attackers will release the potentially sensitive or embarrassing data publicly.

For all organizations that collect, used, and disclose personal information for a commercial purpose, Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA") imposes a range of obligations, including requirements to plan for data breaches, limit their scope should an incident take place, determine the risk of harm to individuals, and notify the federal Privacy Commissioner and affected individuals in certain circumstances. Failure to comply with these requirements can result in significant regulatory fines.

For hospitals or other healthcare providers, Nova Scotia's *Personal Health Information Act* ("PHIA"), imposes additional obligations to implement certain practices to protect personal health information on all organizations acting as custodians of personal health information. Under section 70 of PHIA, if a custodian of personal health information believes that the information they hold has been breached or there is the potential for harm or embarrassment to result, they must notify that individual as soon as possible as per section 69. Failure to protect personal health information as required under PHIA is an offence punishable by a fine of up to $50,000.00 for a corporation, or a fine of up to $10,000.00 (and up to six months imprisonment) for an individual.

Ransomware: The Best Offence is a Strong Defence

There are a number of steps that organizations can take to protect against ransomware attacks and privacy breaches:

1. Work with your IT team to implement regular cybersecurity audits of all critical systems and include mandatory patch updates to all programs.
2. Begin (or increase) cybersecurity training for staff to teach them to recognize malicious emails and phishing attacks.

3. With the assistance of external legal counsel, develop and implement a data incident management plan to identify key leadership roles during the organization's response, outline the necessary risk assessment and notification process, and rollout crisis communications tools.
4. Regularly exercise and test all operational data incident management plans.
5. Back-up systems regularly to limit the risks associated with a data breach.
6. Talk about how your organization will respond if faced with a ransomware attack and come up with a plan. It's easier to develop a strategy before something happens than during a crisis.

The Cybersecurity and Data Privacy Group at Cox & Palmer is happy to assist organizations as they consider and review the risks arising from ransomware attacks.