RISK INSIGHTS

MACKAY
Corporate Insurance Brokers

The Overlooked Physical Exposures of a Cyber-attack

More than ever before, organisations are aware of the potential financial impact of a cyber-attack. Many wrongfully assume that the steep, monetary burden of a cyber-attack (exacerbated by new, higher fines under the GDPR) is exclusively tied to damaged digital assets, lost records, and the price of investigating and reporting a breach. While those expenses represent a considerable hit, damage to an organisation's physical assets can be just as harmful.

Cyber-attacks that cause physical damage typically occur when a hacker gains access to a computer system that controls equipment in a manufacturing firm, refinery, power station or similar operation. After the hacker gains access to an organisation's machinery, they can then control that equipment to damage it or other property.

These types of events can lead to major disruptions and costly damages. To safeguard their physical assets, it's critical that organisations understand what types of businesses and assets are exposed to these attacks.

What's at Risk?

To better understand what kinds of physical losses can occur following a breach, it's helpful to compare cyber-attacks to a natural disaster or other industrial accident. Following these kinds of incidents, organisations often incur costs to repair and replace damaged equipment in addition to any lost revenue caused by the disruption.

Unlike natural disasters, however, cyber-attacks that cause physical damage aren't limited to a geographic location and can impact an entire network. This means that damages caused by a breach can be widespread, affecting multiple sectors of the economy depending on the target.

Because of this, cyber-attacks that cause physical damage are often dynamic and extensive. When an attack on critical infrastructure occurs, it not only affects business owners and operators, but suppliers, stakeholders and customers as well.

Many wrongfully assume that the monetary burden of a cyber-attack is exclusively tied to damaged digital assets, lost records, and the price of investigating and reporting a breach.

Who's at Risk?

Cyber-attacks that cause physical damage—the targets, the assailants, the motivations and the means of the attack—are constantly evolving. Incidents can occur in a variety of ways, including phishing scams, internet exchange point attacks, breaches of unsecured and unencrypted devices, and even plots carried out by rogue employees.

When discussing these attacks, many experts cite power and energy sector organisations as the most at risk. However, vulnerabilities also exist in utilities, telecommunications, oil and petrol, petrochemicals, mining and manufacturing, and any other sectors where industrial control systems (ICSs) are used.

ICSs are open computer systems used to monitor and control physical processes as well as streamline

operations and repairs. ICSs are not often designed with security as a primary consideration, which leaves them susceptible to attack. What's more, for many automated processes, attacks don't even need to cause physical damage to result in significant disruption and losses.

So, when it comes to the emerging risk of cyber-attacks that cause physical damage, targets vary by industry and the damages can be extensive due to the interconnected nature of ICSs.

Real-world Examples

Because organisations are not always required to make cyber-attacks that cause physical damage public, they largely go unreported. However, the following are a number of high-profile incidents that demonstrate how important it is to consider physical and infrastructure cyber-exposures:

- **Ukrainian power grid attack**—This was a multistage, multisite attack that disconnected seven 110 kilovolt (kV) and three 35 kV substations. Together, the attack resulted in a power outage for 80,000 people and lasted for three hours. Using only a phishing scam, the attackers were able to cause substantial, prolonged disruption to the economy and general public.

- **Saudi Arabian computer attacks**—In these incidents, hackers destroyed thousands of computers across six organisations in the energy, manufacturing and aviation industries. Through a simple virus aimed at stealing data, computers were wiped and bricked. Not only did this mean critical business data was lost forever, but all of the damaged computers had to be replaced—a substantial fee for businesses of any size. This attack was similar to an attack on Saudi Aramco, the world's largest oil company, which destroyed 35,000 computers.

- **Petrochemical plant attack**—This attack targeted a Saudi Arabian petrochemical plant. The attack was unique in that it wasn't designed to steal data, but rather sabotage operations and trigger an explosion. The only thing that prevented an explosion was a mistake in the attackers' computer code. Had the attack been successful, the plant would likely have been destroyed and many employees could have died. Experts are concerned that similar attacks could be carried out across the globe.

- **Hospital ventilation attack**—In this incident, a hacker was able to damage and control a hospital's heating and air conditioning system using malware. This attack put the safety of staff, patients and medical supplies in jeopardy, as the hacker could control the temperature of the facilities at will.

Attacks causing physical damage will likely become increasingly common as technology advances and hackers continue to get more creative. Even more concerning is that these kinds of attacks not only endanger a company's data, reputation and finances, but human lives as well.

How Do I Protect My Organisation?

Insurance cover for cyber-attacks that cause physical damage is still in its infancy, and your organisation may have gaps in protection. Even if your commercial property insurance policy includes physical or non-physical damage covers, that does not necessarily mean you're covered from first- or third-party losses from cyber-attacks.

The level of protection your company has depends largely on the structure of your policies. As such, it's critical for businesses to do their due diligence and understand if their policies do the following:

- Impose any limits on cover, particularly as it relates to physical damage of tangible property
- Cover an attack and any resulting damages
- Provide contingent cover for attacks that aren't specifically targeted at the organisation

The Overlooked Physical Exposures of a Cyber-attack

While it's important to speak with a qualified insurance broker about your cyber-risk policy options, there are a number of steps businesses can take by themselves to protect their physical assets. In addition to implementing a cyber-risk management plan, businesses should consider doing the following to protect their data:

1. Keep all software up to date.
2. Back up files regularly.
3. Train employees on common cyber-risks and what they should do if they notice anything suspicious.
4. Review your exposures and speak with your insurance broker to discuss policy options for transferring risk.

For more cyber-related content, contact MacKay Corporate Insurance Brokers today.