CYBER RISKS

IN INDUSTRIAL CONTROL SYSTEMS

OCTOBER 2015

NAS insurance
Specialty Made Simple™

Cyber Liability Beyond Data Security and Privacy

In a world of increased business automation, often the greatest cyber risk companies face is not data security. Rather, businesses that rely upon computers and software to manage their refineries and pipelines, power grids, and a wide range of manufacturing systems face enormous cyber risk should their control systems fail. Though the media and regulatory agencies have not necessarily classified these failures (and their related consequences) as "cyber" incidents, from an insurance and risk management perspective, these failures may be classified as "cyber" risks and considered as covered perils by a cyber liability insurance policy.

Together with our partners at Stroz Friedberg, we collectively wanted to move the commercial cyber liability discussion forward, beyond data breach and privacy, to prompt the industry to embrace a wider interpretation of the cyber risks that companies face. Clearly, data security is a real concern and has become a top priority for executives in every industry. Yet, as privacy breaches grab headlines today, we recognize that there is a much larger cyber security risk looming that insurance companies, risk managers and regulators must now address.

In the following report, we aim to illustrate the risks of industrial control systems with recent real-world incidents across a range of industries including manufacturing, energy and related infrastructure providers. To simplify terminology in this paper, we will refer to the broad range of systems as "industrial control systems," recognizing that there are many names and niches of systems that may elsewhere be referred to as SCADA (supervisory control and data acquisition systems), DCS (distributed control systems), PCN (process control networks) and PLCs (programmable logic controllers). Our intent is not to delve into the vulnerabilities of each of these types of systems. Rather, our goal is to shine a light on the pervasive use of these systems and the risks they present to the companies that employ them.

With a more common understanding of industrial control systems, greater knowledge of recent system failures and a broader recognition of the security risks, we hope this report will not only stimulate discussion, but improve risk management practices among the software engineers, corporate executives and regulatory agencies that collaborate on the design and implementation of these essential infrastructure control systems.

It's not a future problem, it's a *now* problem.

Industrial Control System (ICS) security concerns are not limited to a single industry. In fact, in our increasingly connected "Internet of Things" world, ICSes are expanding beyond traditional industries such as public utilities and manufacturing, to areas such as healthcare, transportation, and even consumer appliances. Some of the more impactful ICS breaches we have experienced recently include:

1. In the summer of 2015, two security researchers[1] demonstrated that attackers were able to gain access to vehicle control systems through the Internet. This access gave them the ability to remotely control a Jeep's air conditioning, radio, windshield wipers, and put the car in neutral. Although this demonstration was non-destructive, it's not hard to imagine that this same access can be used to control safety systems such as brakes, transmission, or engine.

   Connected vehicle systems, such as the GM OnStar system, have been around for quite some time, but as vehicle manufacturers race to turn their cars into smart phones, this concern is bound to increase. While this particular hack has led Chrysler to recall 1.4 million vehicles, this concern is by no means limited to Chrysler vehicles.

2. In late 2014, it was reported[2] by Germany's Federal Office for Information Security that a German steel mill was attacked by sophisticated threat actors who reportedly used a spear phishing exploit to gain access to the corporate network, and then moved laterally through the network into the control systems environment. A blast furnace was managed by one of the targeted ICSes, which was programmed to prevent it from shutting down in a regulated manner, causing massive but unspecified damage to the mill. It is rumored that a Chinese entity caused massive chaos at the German plant to reduce a competitive threat to one or more similar Chinese companies. Reduced steel demand globally, and financial pressure on Chinese steel mills lends credence to this rumor[3].

3. In 2015, security researchers[4] were able to demonstrate that a security vulnerability in a hospital blood gas analyzer device was exploited to pivot into the larger hospital network and obtain patient medical records. Medical devices are especially vulnerable to exploitation because these highly-regulated control systems are often built on operating systems that cannot be patched or updated without violating the manufacturer's warranty, and/or potentially putting the devices out of government compliance. This leads to a situation where the devices must remain in operation with known cyber vulnerabilities.

   While this particular attack observed how a medical device was used to pivot into the hospital network to obtain sensitive information, the researchers also showed that the device's configuration could be changed, leading to false blood readings and affecting patient care. A large variety of medical devices

[1] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014 .pdf?__blob=publicationFile (German language report)
[3] http://www.cnbc.com/2015/03/22/stricken-china-steel-mills-look-to-state-to-ease-exit-strategy.html
[4] http://deceive.trapx.com/AOAMEDJACK_210_Landing_Page.html

are built upon similar foundations and are hence also vulnerable to exploit, such as X-ray machines, MRI machines, Lasik surgical machines, picture archive and communications systems, and infusion pumps. The risk to patient safety is significant.

4. There are several examples of ICS attacks targeting electric, oil/gas, and water utility systems, such as the Maroochy Shire[5] incident in Australia and Stuxnet in Iran, and multiple attacks with no identified victim such as the Havex Trojan[6] and BlackEnergy[7] malware. Utility attacks are especially concerning given that ICS compromise or failure can extend beyond service disruption to environmental impact and safety. For example, the San Bruno gas explosion, while not proven to be a result of malicious activity[8], showed that SCADA (supervisory control and data acquisition systems) deficiencies can contribute to massive system failure and loss of life.

Each of these incidents illustrates the wide range of cyber risks associated with the growing application of automated systems and the broader interconnectedness of infrastructure, devices and industries that relate to our daily lives. In addition, the impact of an incident at this level extends well beyond the host company to affect a much wider radius of related companies and individuals. In the following section, we'll explore specific means of managing cyber risk through effective operational planning and collaborative systems design.

[5] http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf
[6] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
[7] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B
[8] http://cpuc.ca.gov/NR/rdonlyres/28720A78-1DC7-4474-B51F-00C5E8BB5069/0/AgendaStaffReportreOIIPGESanBrunoExplosion.pdf

Why Cyber and Property Policies Need to Work Together

When we think about managing industrial control systems' security risk, we contemplate the first party risks as well as the *downstream* or third-party liabilities.

Focusing on first-party concerns, we consider the large variety of potential threats so that we may consider likelihood, vulnerability, and impact as we build an overall risk profile. Threat actors, or the entities that have the ability to cause harm, consist of several different types of insiders and outsiders, including:

1. Disgruntled employees and/or contractors who have inside access to a sensitive environment
2. Privileged employees and/or contractors who have special access, and whose potential for damage is much greater than a typical user
3. Malicious insiders who are not authorized to be in the building, and who cause physical damage or connect to the network
4. Malicious outsiders such as criminals, hacktivists, and nation states, who attempt to exploit vulnerabilities in systems or people
5. Accidental actions by regular or privileged insiders who have the potential to do significant damage, but without a malicious intent

Equally important for organizations to consider are the third-party or 'downstream' risks that a breach of their environments can pose to their customers, partners and supply chain. A control system disruption can create liabilities that are not necessarily covered by a property policy and lead to a major economic loss. For example, these are some types of downstream risks that should be very concerning to companies:

- A cyber-attack on a networked medical device directly causing or leading to patient harm
- A manufacturing plant's system shut-down that disables the facility from delivering product to its customers (in violation of a service level agreement)
- A power utility disruption affecting operations of hundreds or thousands of customers in a region

These downstream risks represent significant third-party liabilities and losses can accumulate rapidly. Considering that the breach or flaw of the industrial control system may be at the heart of the incident, the property coverage may exclude it. Therefore, the cyber liability policy plays an essential role in risk transfer and cyber risk management becomes an essential practice for the organization.

Effective Cyber Risk Management Begins with Effective Organizational Management

In organizations that have both Information Technology (IT) and Operational Technology (OT) environments, there has traditionally been a split between the people responsible for each – there is often a different skill set required for each environment, and we have seen companies where the organizations do not communicate, and have even seen companies where there is mutual suspicion and distrust between the groups. It won't come as a surprise that an effective risk management program needs to consider the needs of both environments, and create a level of unification necessary to address the risk management needs of the overall enterprise.

In 2012, the US Department of Energy published[9] a risk management process guideline for the electric sector specifically to take a holistic view of risk management between IT and OT environments, and meet the needs of enterprise security risk governance, business process, and technology.

As outlined in the DOE report, the basis of a good risk management process involves four major elements of a risk management lifecycle (see Figure 1):

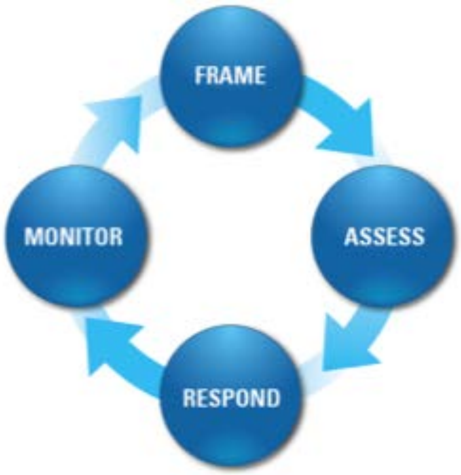


Figure 1: Risk Management Cycle (Source: Department of Energy)

1. **Risk Framing**– understanding the environment in which risk-based decisions will be made, such as business priorities and existing risk assumptions; constraints such as legal, regulatory, budget, personnel, timing; risk tolerance and culture; internal and external relationships.

2. **Risk Assessment** – evaluating the extent to which the existing security program meets all the needs identified in the framing step, and analyzing gaps.

3. **Risk Response** – Planning and implementing the measures necessary to close any identified gaps in the existing security program.

[9] http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp

4. **Monitoring Risk** – Verifying on an ongoing basis that the response measures satisfy the security risk management needs, including monitoring changes in the business and technical environment that may require a reframing of risk.

To further illustrate the point, the following provides an example of a security control assessment for an electric utility that identifies effective risk management processes in design, engineering, and policies that can mitigate system failure and a comprehensive incident response program should a system failure occur.

CASE STUDY: Security Control Assessment at an Electric Utility

Stroz Friedberg was retained to test the corporate and control center networks' resistance to cyber-attack. We also tested the efficacy of key security controls within the utility environment, and reviewed their overall architecture for any resilience improvements and opportunities to reduce recovery time.

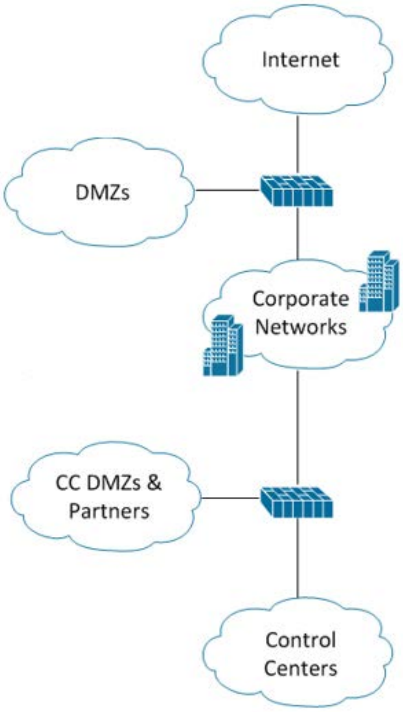
Results:

We found that the utility has a large number of process and technical security controls to protect both the IT and OT environments. Our testing revealed that controls were effectively implemented to protect desktops, servers, network devices, and control center security perimeters. Further, we found that the utility's incident response program is among the best we have seen, including these key elements:

1. A dedicated core response team, with the ability to draw from other departments as needed.
2. A robust protocol to manage the incident response work flow.
3. A robust layer of sensors to detect incidents from a variety of sources, and the ability to quickly retrieve logs and make them available to analysts who are investigating an incident.
4. The company's executive staff takes cyber security seriously and is responsive to requests from the security team.

We also reviewed the utility architecture to improve resilience, limit the effects of a breach, and reduce the time to recovery. This involved our creating a model simulation of the client network in order to assess the network's adherence to security configuration standards[10], and to simulate threats to the network. We also focused this portion of our effort on assessing both preventative and detective capabilities within the infrastructure. The utility segments their network as shown in Figure 1:

[10] Such as the insecure storage of credentials, or the presence of clear-text management protocols



Several key controls are in place to isolate security zones and strictly limit the permitted communications between zones, including:

- Firewalls between zones to enforce security policy in both directions
- A patch management system that rapidly deploys critical security patches to affected systems within each zone, to the extent the patch does not impact system operation
- Secure configuration standards for all servers, workstations, and ICS systems
- System and network-based malware protection to the extent it does not impact system operation
- Network security monitoring to detect the presence of anomalous activity within and between zones

We recognize that systems will always have some level of vulnerability, however our experience teaches us that these standards and practices have helped organizations mitigate risk of a breach and enable rapid, effective response in the event of an incident.

Evolving Cyber Risk Assessment (and Underwriting!) to Meet Demands of Control Systems Cyber Risk

The comprehensive security assessment outlined above goes well beyond current insurance underwriting due diligence and provides a valuable model for risk managers and insurers to consider. The assessment provides a valuable analytical framework and highlights specific areas of IT and OT risk that need to be understood to create an effective cyber risk management plan.,

Working together with their insurers, corporate risk managers can assess their industrial controls systems' cyber risks and develop a cyber risk insurance program that includes the following steps:

1. Evaluate corporate IT and plant systems architecture
2. Assess relationship of Information Technology and Operational Technology personnel, procedures and policies
3. Audit security policy controls (including disaster recovery plans, monitoring and alerting of various security events, on-going vulnerability management)
4. Evaluate the company's Incident Response Plan
5. Account for the potential downstream economic impact of a breach

While each environment will have unique requirements, the approach to assessing cyber risk can borrow from broader security assessments and enable the risk management team to make more informed decisions.

Collaboration is Key For Addressing Control Systems Cyber Risk

Cyber liability insurance is expanding at a rapid pace. The risks, the insurance coverage components and the range of related cyber security services are also evolving at remarkable speed. It's as if Moore's Law is stimulating a similar condition in the growth of cyber risks and insurance solutions!

Through the process of developing this white paper, we recognized that the key to addressing such a fast-moving risk is constant collaboration among key cyber security stakeholders:

- Industrial control system engineers (and related professional associations)
- IT Security professionals
- Corporate risk managers
- Insurance brokers
- Insurance carriers

Our work with Stroz Friedberg, for example, brought to light an effective risk management framework that can be extended to insurance underwriting for industrial control systems cyber risk. We've been able to identify several best practices of organizations that maintain strong security policies and procedures and can now use that information in our own underwriting practices.

With these insights, we believe that even the process of applying for cyber liability insurance can benefit companies and help them identify vulnerabilities in their organization. In addition, as best practices become shared and companies become more familiar with the cyber underwriting process, we would hope that greater preparedness would lead to more favorable insurance rates and thus companies would be motivated to develop a more secure infrastructure.

We hope that this white paper has prompted you to consider the broader cyber risks facing companies and helped you to identify new opportunities for improving your cyber security programs and risk management efforts.

For more information, please contact:

NAS Insurance
Jeremy Barnett, SVP Marketing
jbarnett@nasinsurance.com
www.nasinsurance.com

NAS insurance

Stroz Friedberg
Dave Dalva, Vice President
ddalva@strozfriedberg.com
www.strozfriedberg.com

STROZ FRIEDBERG