PRESENTING OT SECURITY RISK TO THE BOARD
Table of Contents

1.0 Executive Overview ................................................................................3
2.0 Framing a BoD Discussion Around OT Security Risk ..............................4
3.0 A Cybersecurity Framework Is Essential .............................................6
4.0 Addressing Regulatory and Compliance Requirements ........................7
5.0 Measuring & Presenting the Maturity of Your OT Security Efforts ........8
6.0 Identifying Key Metrics to Present to Your BoD ..................................10
7.0 Modeling Potential Financial Losses ..................................................11
8.0 Cyber Insurance for ICS/OT ...............................................................12
9.0 How to Organize Security Governance Across Both IT & OT .............13
10.0 Presenting OT Security Risk to Your BoD .........................................14
11.0 Summary ............................................................................................15
Endnotes ....................................................................................................16
Operational Technology (OT) networks were traditionally kept separate, or “air-gapped”, from IT networks. However, new business requirements associated with the efficiency benefits of digitalization, such as smart environmental control systems, just in time manufacturing, and interactive systems tied to Big Data, are forcing increased connectivity between IT and Operational Technology (OT) networks, thereby increasing the attack surface and hence the cyber risk.

In fact, many of today’s OT networks are transited or tunneled over corporate networks, leverage common internet protocols, run on general-purpose hardware and mainstream operating systems, and are increasingly connected via wireless technologies. As a result, the hardware and software that monitor and control physical equipment and processes for critical infrastructure present a wildly attractive target for those who seek to cause disruption or to threaten infrastructure for their own purposes.

One growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the essential systems that keep societies functioning (electricity, telecommunications, water, transportation, etc.).

Protecting OT networks is a challenge. While some OT networks may have similarities to IT networks – and lend themselves to the traditional types of security measures used to protect them, such as SIEMs and firewalls – there are many characteristics of OT networks that differ from traditional IT systems. Differences include specialized protocols such as Modbus for PLCs, difficulties with patching systems that run 24/7, legacy embedded devices with proprietary architectures, differences in network behavior, and long equipment replacement cycles. Therefore, simply transferring security processes and technology from IT to OT will not succeed in protecting your OT networks.

The risks associated with OT networks also differ — and they need to be understood by your Board of Directors (BoD). These include significant risks such as costly production outages leading to financial losses, catastrophic safety failures and environmental damage leading to potential liability issues, and theft of corporate IP leading to loss of competitive advantage.
2.0

Framing a BoD Discussion Around OT Security

A key goal of the BoDs of most enterprises is to maintain an appropriate balance between protecting the security of the enterprise and its ability to function, and controlling financial outlays from losses.

They care about “strategy – not operations,” “risk oversight – not risk management,” and “business outcomes – not technology details.”

And regarding your OT networks and potential security risks, they likely have 5 specific asks:

1. To understand and (be able to) approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue

   The domains of IT and OT are different, and they have different risk appetites and functional requirements. Not only are the appetites different, the dimensions of the risk are different. In the IT domain, confidentiality is usually key. In the OT domain, the focus generally centers on safety and reliability. OT devices typically interact with the physical world; therefore, events in the digital world may affect the physical world. This may harm human life and the environment.

2. To understand the legal implications of cyber risk as they relate to the enterprise’s circumstances

3. Adequate access to cybersecurity expertise, (and agreement) that cyber-risk management will be given regular and adequate time on board meeting agendas

   Creation of a Technical Advisory Board consisting of content-knowledgeable staff from IT and OT can help address this ask

4. To set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget

   Establish accountability, responsibilities and authority – a combined governance body can set the roles, responsibilities and the authorities of all resources in the enterprise, regardless of whether it’s involved in the IT/OT security realm. This will reduce the chance of conflicts and enable more-optimal resource use.
5. Commitment that any discussions about cyber risk will include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Align risk appetite — a single governance body can agree on a common risk appetite for integrated IT/OT environments. Alternatively, a tiered approach is adopted, and different levels of risk are agreed on, accepted and documented per domain.⁹

In addition, if you are going to be personally engaging with your BoD, the US Department of Homeland Security (DHS) suggests there are six questions you should be prepared to answer:

**Question #1: What’s at risk** — are assets prioritized and potential consequences identified if our ICS is compromised? Can we sustain operations of critical processes following a cyber incident?

**Question #2: Who is ultimately responsible** for cybersecurity?

**Question #3: Is there Internet connectivity** to our ICS environment? If no, how did we validate that fact?

**Question #4: Is there remote access** to our ICS network? If so, why, and how is it protected and monitored?

**Question #5: Do we have a DHS HSIN account** to receive alerts and advisories?

**Question #6: Are best practices being applied?**³⁵
Presenting OT Security Risk to the Board

3.0

A Cybersecurity Framework is Essential

Ideally, in any discussions with your BoD regarding OT security risk you will be able to describe your OT cybersecurity efforts in the context of a cybersecurity framework based on OT industry best practices. Many different frameworks exist, including some that are tailored to specific OT environments such as electricity, oil and gas industries.

In the US, the Cybersecurity Enhancement Act of 2014 (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators.

The resulting NIST ‘Framework for Improving Critical Infrastructure Cybersecurity’ focuses on using business drivers to guide cybersecurity activities and consider cybersecurity risks as part of the enterprise’s risk management processes.

The NIST Cybersecurity Framework was designed to be modified based on your needs – including industry-specific regulations that often drive behavior and mandate certain security requirements.
4.0

Addressing Regulatory and Compliance Requirements

The growing number and sophistication of cyberattacks on industrial and critical infrastructure have led legislators in the US and EU to mandate adherence to several industry and governmental regulations. These include the North American Electric Reliability Corporation (NERC), the US Nuclear Regulatory Commission (NRC), the EU Network and Information Security Directive (NISD), and more.

Of the various regulations, NISD has the broadest impact as it applies to enterprises that provide "essential services" in critical infrastructure sectors such as energy, transport, water, health sector, banking & financial, and digital infrastructure (ISPs, CDNs, DNS, etc.). Additionally, enterprises in other sectors such as manufacturing, pharmaceuticals, chemicals, and oil & gas are voluntarily leveraging the NISD guidelines as a framework for improving their operational resilience.

NISD is the first regulation to define "minimum standards of due care" for protecting OT networks. This means that in the case of a major safety or environmental incident, enterprises may be held negligent and financially liable for not having taken minimum steps to prevent it – even non-EU enterprises.

Many US organizations will also be affected by NISD because they have operations in the EU. NISD sets a compelling precedent that non-EU enterprises should consider following voluntarily, even if they are not currently legally bound by the Directive’s requirements.
As with security frameworks, there are many approaches available to build a model that measures the maturity and success of your security efforts. A capability maturity model provides a benchmark against which an enterprise can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. In its simplest form, each line item deliverable from your cybersecurity framework is evaluated against a pre-defined set of criteria to determine the level of maturity in which the initiative is operating.

When a model is widely used in an industry an enterprise can benchmark their performance against other enterprises. This is especially useful when presenting to your BoD.

One example is the ‘Cybersecurity Capability Maturity Model’ (C2M2) created by the US Department of Energy (DOE) in partnership with the US Department of Homeland Security (DHS). As stated in their guidelines, “the C2M2 focuses on the implementation and management of cybersecurity practices associated with the information technology (IT) and operations technology (OT) assets and the environments in which they operate.

The model can be used to:

- Strengthen enterprises’ cybersecurity capabilities
- Enable enterprises to effectively and consistently evaluate and benchmark cybersecurity capabilities
- Share knowledge, best practices, and relevant references across enterprises
- Enable enterprises to prioritize actions and investments to improve cybersecurity”
A maturity model that combines the NIST Cybersecurity Framework and the DOE C2M2 might look as follows:

<table>
<thead>
<tr>
<th>Establish Cybersecurity Risk Management Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL1</td>
</tr>
<tr>
<td>MIL2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>MIL3</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

### Mapping a Maturity Model to a Cybersecurity Framework

<table>
<thead>
<tr>
<th>OT Cybersecurity Capability Maturity Model</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td><img src="https://via.placeholder.com/15" alt="Green" /></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td><img src="https://via.placeholder.com/15" alt="Yellow" /></td>
</tr>
<tr>
<td>Risk Management Strategy</td>
<td><img src="https://via.placeholder.com/15" alt="Green" /></td>
</tr>
<tr>
<td>Protect</td>
<td><img src="https://via.placeholder.com/15" alt="Yellow" /></td>
</tr>
<tr>
<td>Detect</td>
<td><img src="https://via.placeholder.com/15" alt="Yellow" /></td>
</tr>
<tr>
<td>Respond</td>
<td><img src="https://via.placeholder.com/15" alt="Yellow" /></td>
</tr>
<tr>
<td>Recover</td>
<td><img src="https://via.placeholder.com/15" alt="Red" /></td>
</tr>
</tbody>
</table>

Presenting the Maturity of a Cybersecurity Framework to a BoD
Identifying Key Metrics to Present to Your BoD

Time, safety and continuation of services are of great importance, since many ICSs are in a position where a failure can result in a threat to human lives, environmental safety, or production output.\(^{16}\)

“Metrics can provide cyber defenders of an ICS with critical insights regarding the system”.\(^{17}\) A good metric is “relevant, unambiguous, direct, operational, understandable, comprehensive”.\(^{18}\)

A critical element in eliciting a meaningful metric is to gather the relevant information about one’s system and to align that metric with measurable goals and strategic objectives which lie within the scope of a given project or the domain of an enterprise structure.\(^{19,20}\) Categories may include enterprise, operational, and technical metrics.\(^{21}\)

Simple metrics might include checks to ensure that employees received appropriate background checks, activation of locked gates, or data being encrypted at appropriate levels.

One source with a wealth of information on this subject is the chapter on ‘Security Metrics in Industrial Control Systems’ in the US Army’s “Cyber Security of Industrial Control Systems, Including Scada Systems” (2016).\(^{22}\) As the saying goes, “what gets measured gets done”.

<table>
<thead>
<tr>
<th>CHARACTERISTIC</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant</td>
<td>Metrics are directly linked to decision-making goals and objectives</td>
</tr>
<tr>
<td>Unambiguous</td>
<td>Consequences of alternatives can be clearly measured by metrics</td>
</tr>
<tr>
<td>Direct</td>
<td>Metrics clearly address and describe consequences of interest</td>
</tr>
<tr>
<td>Operational</td>
<td>Data exist and are available for the metric of interest</td>
</tr>
<tr>
<td>Understandable</td>
<td>Metrics can be understood and communicated easily</td>
</tr>
<tr>
<td>Comprehensive</td>
<td>The set of metrics address a complete suite of goals and consequences</td>
</tr>
</tbody>
</table>
Presenting OT Security Risk to the Board

7.0

Modeling Potential Financial Losses

“Cyber-attacks on industrial control systems (ICS) that underpin critical infrastructure can be characterized as high-impact, low-frequency events. To date, the volume of attacks versus the overall global footprint of ICS is low, and as a result there is an insufficient dataset to adequately assess the risk to an ICS operator, yet the impacts are potentially catastrophic.”

And the fact that the volume of attacks is small does not mean they are insignificant. In June 2017, the Russian military launched the cyber-attack now known as “NotPetya” that resulted in billions of dollars in losses across Europe, Asia, and the Americas. Enterprises experiencing massive financial losses included Merck ($915M); FedEx ($400M); Saint-Gobain ($255M); and more. AP Moller-Maersk took a $300M loss that included replacing 45,000 PCs, 4,000 servers, and installing 2,500 applications.

Creating a model that clearly identifies the potential financial risks of a cyber-attack on your ICS/OT environment is critical. Given the nature of ICS/OT environments the model is likely to be unique to your enterprise. One approach is to utilize the guidelines proposed by Kaplan and Garrick (1981) who postulated that a risk could be described by answering three questions:

1. What can happen? (i.e., what can go wrong?)
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

Answering these questions with techniques used to model other financial aspects of your enterprise – or one of many others identified in ‘Measuring the Risk of Cyber Attack in Industrial Control Systems’ – will enable you to present your BoD with a financially-based position statement regarding the importance of securing your ICS/OT assets.
Cyber Insurance for ICS/OT

One of the responsibilities of a BoD is to transfer risk inherent in operating an enterprise. That is often done through the purchase of insurance policies from 3rd-party enterprises. Not surprising, “retailers, banks, and healthcare providers began seeking out cyber insurance in the early 2000s, when states first passed data breach notification laws. But even with 20 years’ worth of experience and claims data in cyber insurance, underwriters still struggle with how to model and quantify unique types of risk.

Recent policies tend to accommodate first-party liability coverage, including costs like online extortion payments, renting temporary facilities during an attack, and lost business due to systems failures, cloud or web hosting provider outages, and even IT configuration errors.”

ICS-specific cyber insurance is also available. However, unlike the predictable costs associated with the loss of personal data, or the relative ease of projecting the amount of revenue lost from an e-commerce site not being available during a specific period, modeling the costs associated with attacks against an ICS and related infrastructure tend to be unique.

As such, the insurance premiums charged to protect against ICS/OT-type losses tend to be very customized – and much higher than IT-related cyber insurance, as it is near impossible in many cases for an insurance underwriter to spread your distinct ICS/OT risks across multiple policy holders.

Therefore, it is imperative that the BoD be provided with a financial model (see previous) that enables them to engage in an informed discussion with insurance providers. This will enable your BoD to decide whether to utilize 3rd-party insurance to transfer risk or self-insure.
How to Organize Security Governance Across Both IT & OT

According to Wam Voster, Gartner Research Director, “Enterprises with both IT and OT struggle with the coexistence of two separate security and risk management functions. This leads to a dispersed view on the overall operational risk the enterprise is facing. In a continuously evolving threat landscape, a single established security and risk management function is better-positioned to address these threats across both IT and OT. A single leader of this function can also be held accountable for the enterprise’s overall digital risk.” This will allow board members to consult only one leader to get a comprehensive view on the digital risk the enterprise is facing.

The owner of this function should be responsible for overseeing an enterprise’s management of cybersecurity including appropriate risk mitigation strategies, systems, processes, and controls.

Gartner refers to this individual as the Digital Risk Officer, the characteristics of which are as follows:

- A business leader, a manager and a communicator, not a technologist
- Work with executive management to determine acceptable levels of risk
- Own governance, roles and responsibilities, and awareness
- Develop a security vision and strategy
- Establish and maintain the combined security program
While it may seem obvious, preparing to present to your BoD should include knowing your audience: Who are they? What is their background? What role do they serve on the BoD? What are their biases and passions?

Keep the presentation short and to the point (Gartner’s Rob McMillan suggests a 7-slide approach), and focus on facts, risks, the future and actionable plans. Topics to be discussed may include:

- **Disclosure of any known threats**, including insider, supply-chain/3rd-party risks, nation-state, etc. and potential business impact for each risk

- **The maturity of your cybersecurity efforts** that includes a mapping of your cybersecurity framework to an accepted capability maturity model. This should include enterprise readiness, areas of most concern, ability to transfer (outsource) risk, etc.

- **Updates on key security metrics** that you are tracking

- **Anecdotes about other enterprises** within your industry that have experienced – and addressed – ICS cyberattacks
There are increasing security risks associated with OT networks, according to the most recent SANS Survey, the current lack of visibility into the security and resiliency of OT networks is far-reaching – with the majority of respondents (59%) stating they are only “somewhat confident” in their organization’s ability to secure their ICS/SCADA infrastructure.

In addition, the increasingly blurred lines between traditional IT networks and OT networks has introduced additional challenges.

Given the potential implications to the health and safety of human lives, environmental damage, financial issues such as production losses, negative impact to a nation’s economy, and in a worst-case scenario the very ability of a society to function, it’s important that OT network security be addressed in a manner like IT network security – including having board-level visibility.

Centralized leadership for both IT and OT security, combined with a security program that incorporates a cybersecurity framework designed specifically for OT networks, along with the appropriate ongoing monitoring and measurement of that program, will help enterprises manage and minimize their OT security risks.
Presenting OT Security Risk to the Board

Endnotes

1. CSO Online - Securing OT Networks Against Rising Attacks
4. NIST Guide to Industrial Control Systems – SP 800-82
5. Gartner – Security & Risk Management Summit 2018 – ‘What Your Board Wants to Know’
10. NIST Guide to Industrial Control Systems – SP 800-82
15. US Department of Energy (2014) – ‘Cybersecurity Capability Maturity Model (C2M2) v1.1’
30. Gartner – Research Note - How to Organize Security and Risk Management in a Converged IT/OT Environment
31. DENTONS – A cybersecurity guide for directors (p. 4)
ABOUT CYBERX

We know what it takes.

CyberX delivers the only industrial cybersecurity platform built by blue-team cyber-experts with a proven track record defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing ICS risk and preventing costly production outages, safety failures, and environmental incidents.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 US chemical company; a top 5 global pharmaceutical company; and national electric and gas utilities across Europe and Asia-Pacific. Strategic partners include industry leaders such as Palo Alto Networks, IBM Security, Splunk, Optiv Security, DXC Technologies, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it’s the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their ICS networks for malware and targeted attacks. What’s more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

For more information visit CyberX-Labs.com or follow @CyberX_Labs.