10 THINGS NOT TO TELL YOUR BOARD ABOUT YOUR OT CYBERSECURITY PROGRAM

Honeywell

Within a corporate Board environment, cybersecurity can be vastly misunderstood and yet remains a critical priority for oversight. Gartner estimates that by 2020, 100% of large enterprises will be asked to report to their Boards on cybersecurity and technology risk[1]. Operational security experts may be called upon by Boards for data, status or perspectives. As Boards increasingly add Technology committees and even Cybersecurity committees to their structures, the need for a balanced dialogue and expertise will only increase.

For those managing complex operational technology (OT) systems and plants, a vital skill is the ability to manage leadership expectations while communicating sensitive situations in a factual and informative manner. By far the most dangerous situation for a security practitioner advising a business group is to misrepresent the level of risk facing an organization. This can open the company up to costly lawsuits and unwelcome publicity, not to mention the direct risk concerns of human safety and environmental damage. Similarly, overreacting on risk can deplete company resources and unnecessarily divert focus.

Managing your operations information flow and approach with leadership can be a positive and mutually beneficial relationship if a few considerations are kept in mind. This whitepaper notes the top ten comments that are best avoided when handling cybersecurity situations with your Board or leadership teams.

"YOU HAVE NOTHING TO WORRY ABOUT." 1

While confidence can be a reassuring leadership trait in certain roles, when it comes to cybersecurity, pretending that risk does not exist is irresponsible. There is always risk, and leadership needs to understand precisely what that risk is in order to make policy and organizational decisions. Communicating that the Board has nothing to worry about completely misses the granular and rich discussion necessary about risk and how to handle it. It is for them to weigh in on what can or should be worried about at the corporate level; masking particular risks can be misleading.

For example, if they are unaware of remote connectivity's impact in an operational setting, they may drive ahead on initiatives that initiate dozens of uncontrolled connections, and they may miss investing in countermeasures and controls that can limit the risk while embracing the opportunity. Rather than stating "you have nothing to worry about," communicate what measures will be needed as part of the initiative, such as "if we need to allow remote connectivity to our mine in Chile, we need to implement monitoring software to record and log those remote sessions and to change our access privileges."

There is always something to worry about in security, and helping leadership understand that makes for a more realistic and balanced risk management discussion. It also allows security to become part of all conversations, rather than an isolated domain disconnected from the organization's key initiatives.

"NONE OF OUR SYSTEMS ARE VULNERABLE."

2

With attackers changing approaches on a minute-by-minute basis, it is impossible to share status that all systems are protected against every vulnerability. Even if you have patched all systems recently, there are still zero-day attacks yet unpublicized, as well as other mechanisms that are always available to attackers. For example, addressing vulnerabilities in an operating system may not address chip vulnerabilities.

Leadership teams need to recognize that there are always outstanding vulnerabilities. Whether it is worth the cost, resource, and hit to production to address these vulnerabilities is part of their oversight responsibilities. As the operational leader, it can be best to describe what categories or areas of vulnerabilities have been addressed in that moment, while making it clear that there can be other unknown risks or a set of liabilities that are intentionally not addressed.

In addition, when it comes to vulnerabilities, Boards are interested in which technology systems contribute to which levels of risk. They may find it helpful to know that 60% of the infrastructure is running on systems with the most vulnerable OS type. They can then decide if it's critical to upgrade those systems, or to accept the risk those systems bring relative to the value they provide to the business. Implying that no systems are vulnerable makes it difficult to plan upgrades or otherwise make trade-off decisions regarding operational infrastructure.

3

"THE PERSON WHO KNOWS THE MOST ABOUT THE CYBERSECURITY OF OUR SYSTEMS LEFT THE COMPANY."

Talent and people with expertise in cybersecurity may be in short supply, and this is well known at Board levels[2]. Rather than find yourself in a situation where key expertise is missing, proactively review resources to clearly articulate to leadership both your high potential and critical talent resources.

Since you will regularly communicate regarding risk, it is important to decipher for leadership which talent relates to which levels of risk. If your organization has stated headcount limitations or other resourcing constraints, it is your responsibility to find other means, such as outsourced relationships or contracted expertise, to address unacceptable levels of risk. This may also be required for compliance, which is a high priority topic for Boards.

When considering your responsibilities for cybersecurity, it can be helpful to broaden beyond technology to ensure people, process, and systems are actively managed relative to risks the company faces. For example, if you only have limited personnel with specific cybersecurity knowledge, consider how to transfer knowledge to others and how to offset the risk that a single individual's departure could impact your cybersecurity program. If you face staffing shortages, plan ahead for augmented expertise or new service contracts with OT cybersecurity partners.

“WE DON’T NEED TO SPEND ANY MORE ON OUR CYBERSECURITY PROGRAMS.”

4

Some surveys have concluded that in the industrial sector in particular, investment in security countermeasures is not on par with levels of risk[3]. For example, there are still organizations that are not even performing any manner of risk assessments (a basic cybersecurity step). In addition, it has been well documented that the nature of OT-targeted attacks is dynamic, and involves ongoing pressure from nation states, activists, competitors and financially motivated hackers.

Considering these pressing “hazardous” conditions, there is always cybersecurity work to be done. With your cybersecurity program, you have your key objectives identified and an ongoing practice that can always apply more resources to offset risk. For example, if your objective is to centralize security operations, there are multiple automation and management software solutions that could be added to expedite remote team data sharing in a secure manner, or solutions to control and monitor access.

Layering in security across people, process and systems is an ongoing practice. Investment should be commensurate with reaching your objectives. Many companies keep an ongoing list of key cybersecurity work as budgets evolve, based on their risk assessment findings or a review of program objectives and status. For example, changing out routers to allow for newer levels of encrypted communication may not be on the first priority order ahead of patching high value servers, but it can be a useful investment should funding become available.

"WE DON'T THINK WE'RE A TARGET."

5

The volume, speed, and dynamic nature of today's threat landscape has led some security experts to suggest that ICS is a target, and recent alerts pinpoint specific risks for industrial control system operators[4]. From local hospitals, to major brands, to water processing facilities to fertilizer makers, every connected organization is at risk of compromise[5]. Trends change, and the nature of threats constantly evolves, from the past denial-of-service waves to today's ransomware campaigns. Rather than diminish the level of risk, clearly identify the company's high value assets, then assume someone will want to target them. Advising that your company is not a target reduces vigilance and starves security resources, leading to greater levels of risk.

To balance the conversation, it is worth discussing what level of effort will be required to protect your organization as a target. For example, if you make farming equipment with remotely controlled tractors, a potential target could be taking over control of those tractors resulting in crop damage or putting operators in danger. Discuss if the organization could tolerate such an incident, and if not (as is likely), direct the conversation toward what obstacles could be layered in to slow down attackers. Through such discussions, Board members often recognize that always assuming they are a target can actually expedite protection. Focusing on not being a target increases risk through omission and can also hold back the organization from modernizing systems and practices.

As the operations leader advising on cybersecurity, it is in your best interest to keep the organization vigilant and on top of security resources at all times. This builds in the assumption that the organization is a target.

"UNLESS WE HAVE THE LATEST TECHNOLOGY, WE DON'T STAND A CHANCE."

6

Technical solutions are indeed an essential part of a cybersecurity program, considering the intricate technicalities that hackers leverage to perform malicious acts. At the same time, engaging people controls and process controls is equally essential for your security posture. Layering in defenses across all of those dimensions can help manage risk. As you communicate with leadership, continually broaden their horizons to consider these three areas (people, process, technology). This approach can support the Board to better balance investments relative to the organization's risk appetite and ability to mitigate threats.

For example, if you overinvest in technology but do not train your personnel how to avoid phishing attacks, you have left open a major avenue of attack. While you may have better automated and streamlined technical controls, you have done little to reduce risk from social engineering, a common and problematic source of compromise. Similarly, having the best technology does not eliminate the need for ongoing risk assessments, which commonly uncover concerning risks such as uncontrolled remote access points or visible passwords posted alongside servers.

All that said, it should be noted that in certain areas, the latest technology updates are a critical part of the cybersecurity practice. For example, when addressing USB-borne threats or exploits of OS vulnerabilities, having an evergreen system of known attacks and mitigations is essential. This does not necessarily require procuring new technology but ensuring a rigorous process for updating existing systems. The main point is to balance the emphasis on technology with the equally important dimensions of people and process investments.

“THE DIFFERENCE BETWEEN IT AND OT SECURITY IS TOO SMALL TO TREAT THEM SEPARATELY.”

7

At the Board level, cybersecurity may be viewed as an umbrella term, much like medicine or law, with little understanding of the vast differences among practitioners and related solutions. As you discuss risk and mitigations, it can be helpful to clarify why particular IT methodologies cannot work in industrial OT settings. This can range from ensuring basic requirements are well known, such as the ability to operate under extremely hot or cold temperatures, all the way to educating about newer risks such as hardening any off-the-shelf Windows servers or adjusting patching schedules to avoid interference with production.

Aligning to IT procedures without protecting against the greatest OT risks will only open the organization up to more liabilities and internal conflict. The voice of OT is essential in guiding security oversight at the Board level, to help match vigilance and investment with the specific type of environments, systems and working conditions of operations.

Similarly, considering people and process concerns specific to OT can help mitigate risk. For example, personnel with ICS security expertise or people approved and trained to work at an offshore platform may be important requirements for OT talent recruitment but not for IT. Rather than simply grouping IT and OT together, advocate for specialized OT compliance or training needs to ensure the company and its customers are adequately protected.

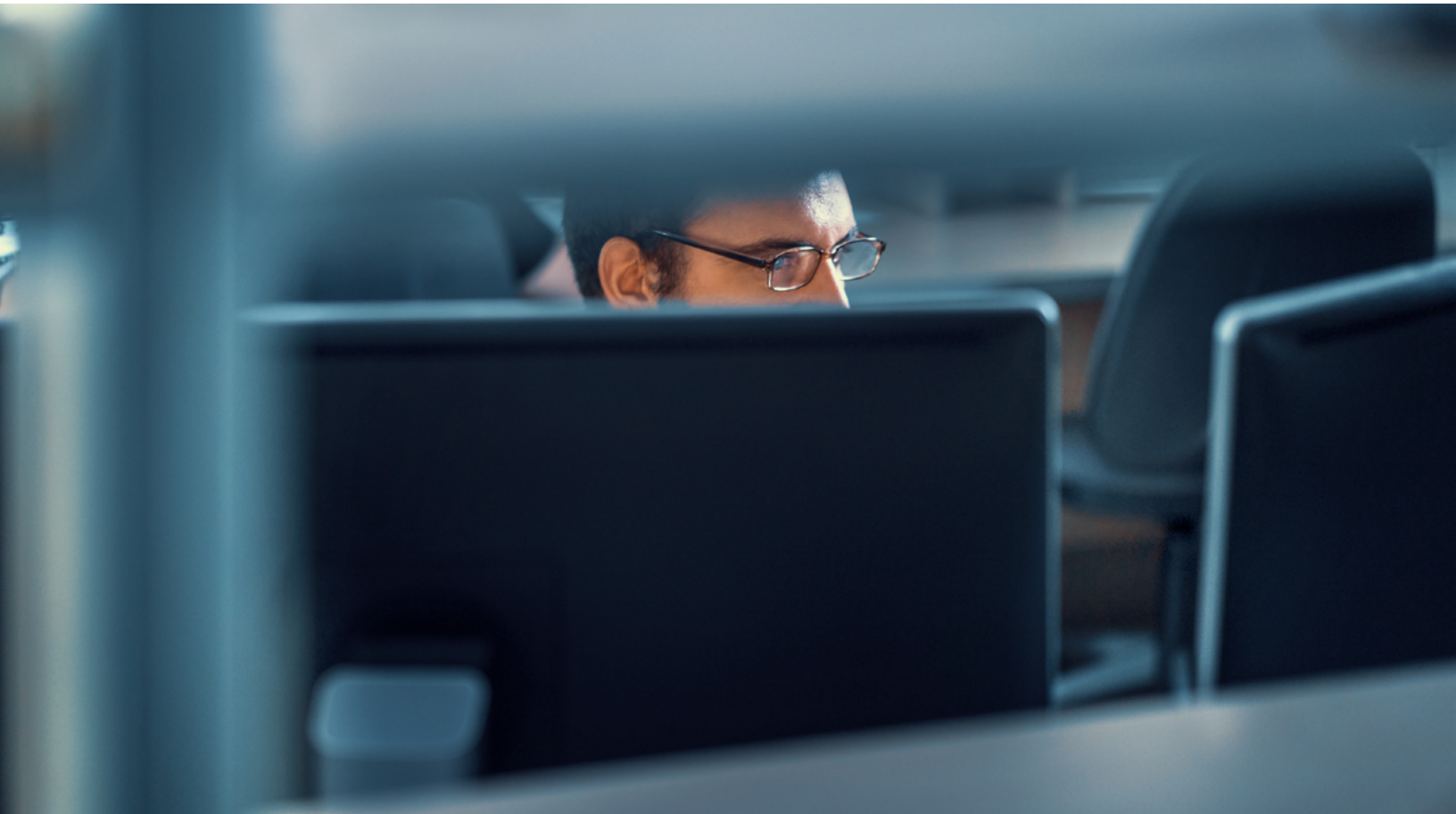
"OUR IT AND OT CYBERSECURITY TEAMS DON'T NEED TO WORK TOGETHER."

8

Similar to voicing the unique requirements of OT, it is in your company's best interest to have dialogue between IT and OT. Especially as the volume of assets in an industrial organization increases, there will be greater scrutiny on security across these devices, as well as inevitable security concerns amidst ongoing digitization. Moving laterally or between networks is increasingly common among hacker techniques, further requiring varied security teams to address threats holistically.

While it can be pragmatic to group categories such as "devices" into a single Board conversation, it is still essential to convey that IT and OT will need to manage such devices differently considering their usage and role within each area. It is also beneficial to work together to secure resources and funding in more cost-effective ways that still honor the differences in requirements.

For example, procuring an outside organization to perform risk assessments can package in different, specialized types of OT and IT assessments under one purchase order, aligning to common Board requests for quarterly reviews. As IT and OT work together to review assessment findings, areas of investment that can support both teams' missions may appear, such as securing patch updates through a secure mechanism from software providers, or personnel training about threats. Rather than duplicate training programs and overloading employees, a combined training can cover both the business network concerns and operational network concerns. This cross-training can also help educate each group about the other while complying with training needs.



"OUR SYSTEMS CHANGE SO SLOWLY OVER TIME, WE CAN AFFORD TO FOCUS EFFORTS AWAY FROM CYBERSECURITY."

9

Legacy systems are not immune from attack. Recent cases have shown nation states targeting critical infrastructure providers, showing little regard for what systems are in place for how long. In addition, as recent high-profile breaches have highlighted, a consistent patching regime for any system is an essential part of ongoing cybersecurity needs. A further trend impacting legacy systems is the global drive toward manufacturing connectivity, seeking to leverage data from devices and systems to optimize performance or gain insights[6]. Often this requires upgrading those systems or adapting them to allow for monitoring or data extraction. These trends increase the risk that older infrastructure will be exploited or disrupted and will thus require ongoing cybersecurity vigilance.

Beyond the direct technical concerns of legacy systems, the organization can never lose sight of the fact that processes and people introduce risk. This has little to do with how slowly systems do or do not change. For example, many processes have been in place for years, and have not been updated to reflect current conditions. An offshore oil rig may have a process that requires opening up a remote connection, inadvertently allowing workers to relax watching a movie after long shifts. Today, that connection can serve as a penetration point to reach other systems on the rig and represents a security risk that requires associated controls. Just as systems are slow to modernize, processes and training programs can be obsolete and introduce risks that must be mitigated to protect the organization.

10

“WE’RE ALWAYS ONE STEP AHEAD OF ANY ATTACKERS.”

While it is prudent to deploy preventative measures as part of your cybersecurity program, response and mitigation investments are equally important. Leadership appreciates models and frameworks such as the NIST Cybersecurity Framework to recognize where and how risk will be addressed. Implying that all efforts in the preventative category will always work every time to stay ahead of attackers is simply naïve. Attackers are often highly motivated, agile, and well resourced, sometimes far more resourced than corporate security teams! Characterizing attackers as less advanced than commercial enterprises can be misleading and can result in poor investment choices and an inaccurate assessment of company risk.

Boards can instead be briefed on any active campaigns, particularly those applicable to their region or industry, and overall threat trend changes and related mitigations. Ongoing risk assessment findings can be shared at a high level, as well as attacks averted. These views into the threat landscape are more realistic to represent the dynamic nature of cybersecurity and to further reinforce its function as an ongoing practice, not a static field. The operations leader can always bear in mind that Boards want to see and manage risk as responsible stewards. They are not seeking sales pitches or rosy pictures that ignore potential risks.

CONCLUSION

Corporate Boards are accountable for the viability and longevity of an organization. Understanding cybersecurity risks is an increasingly common need for Boards globally. Through a balanced conversation across people, process and technology needs, together with established standards and frameworks, operational experts can engage with Boards as informed and valuable leaders. Avoiding common mistakes such as mispresenting risk, avoiding risk mentions, or not protecting OT specialized requirements can support a positive ongoing relationship to steer an organization through today's complex digital environments.

SOURCES:

(1) https://www.gartner.com/en/information-technology/insights/cybersecurity

(2) https://www.directorsandboards.com/articles/singledriving-focus-risk

(3) LNS Research: https://www.honeywellprocess.com/en-US/news-and-events/Pages/pr-12062017-honeywell-survey-shows-low-adoption-of-industrial-cyber-security-measures.aspx

(4) https://www.zdnet.com/article/ransomware-attacks-are-now-targeting-industrial-control-systems and https://securityledger.com/2018/10/report-obvious-security-flaws-make-ics-networks-easy-targets

(5) Hospitals: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far
Water: https://www.eenews.net/stories/1060131769 | Chemical: https://www.securityweek.com/major-us-chemical-firms-hit-cyberattack

(6) https://www.cloudcomputing-news.net/news/2019/jun/26/how-cloud-transforming-manufacturing-and-financial-services-2019

For more information

To learn more, visit:
www.becybersecure.com or
contact your Honeywell
Account Manager, Distributor
or System Integrator.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, GA 30308
www.honeywell.com

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell