Perspective

DEVELOPING AN INDUSTRIAL CYBER SECURITY STRATEGY

Shouldn’t you have a strategic plan to protect your most strategic assets?

Two years ago, I began my new career in industrial cybersecurity when I joined Verve Industrial Protection as CEO. I had spent the past twenty years at McKinsey & Co, the world’s leading strategic management consultancy, serving large organizations on their most critical strategic issues. There I learned the importance of analyzing opportunities and threats, building data-based perspectives on options, making hard choices on priorities, building "strategic horizons" of investments over time, building staff, systems and skills to support the strategy, etc.

Since joining Verve, I have come to realize that these same skills and approaches are as critical to cybersecurity as they are to other elements of a company's business. But all too often, this issue is not approached with the same "strategic toolkit" that is used in other areas of business. For some reason, cybersecurity is often treated as more of a nagging problem that just needs to be "handled" rather than a strategic issue for the C-suite or board of directors.

What is most striking about the "strategies" that are in use, is that most of them focus exclusively on the "information" assets of companies – employee and customer records, information systems, IP, etc. In large part this is because the public incidents – to date – have been focused almost exclusively on these assets. The assets that control the delivery of supplies, manufacturing or delivery of products & services are often either forgotten or excluded for a variety of reasons: lack of compliance requirements, lack of recognition of the risk, and lack of a plan to remedy.

Over the past two years, we at Verve have built an approach that brings great toolsets from the likes of McKinsey to the world of cybersecurity to help drive dramatic improvements in risk reduction while reducing the overall cost of a program. One of the most significant implications of this approach is to reset cybersecurity priorities to focus more attention on the "operating technology"[1] or control systems rather than on traditional "information systems". We are confident that such an approach can dramatically increase the ROI of a company's cybersecurity program – and provide the C-suite and board of directors a way to assess progress in a way that is similar to how they discuss other strategic issues.

In the below whitepaper we lay out the five key steps to building an effective cybersecurity strategy.

1. Identify where to compete: Define which assets and networks are most critical to your overall business strategy, where the risks are greatest, and prioritize where to focus on those areas. In many cases we find that the operating technology – i.e. those computer systems that control manufacturing, supply chain, service delivery, etc. are often ignored by traditional cybersecurity approaches.
2. Set aggressive, clear and measurable targets: Establish a set of metrics - likely based on one of the available cybersecurity standards – against which you can measure progress and ROI
3. Establish clear budgets: successful strategies require the right resources, but cybersecurity budgets are hard to set because they are often hard to measure. By establishing measurable targets in step 2, this should allow for clearer budgeting and planning discussions.
4. Define "how to compete": Create a programmatic "portfolio of initiatives" that work together to improve your security fabric as additional initiatives and solutions are deployed

[1] Operating Technology refers to the technology that facilitates the safe, reliable, expected operation of a production facility. This often includes 'tradtional' technology like windows or OS based devices but also means embedded or control system equipment like relays, PLCs and controllers.

5. Build or buy: Decide where you can be truly distinctive and where third parties can provide greater scale or distinctive knowledge. Focus internal resources on critically strategic capabilities and outsource other, less strategic elements

These steps – taken from the basic tenants of business strategy research over the past 80 years – can create a clear, high return cybersecurity strategy that will both drive improved results as well as provide visibility to critical C-suite and board of directors' stakeholders.

Step 1: Where to Compete

Compete may seem like an odd word to use when discussing cybersecurity strategy. We believe, however, that the notion is very applicable in today's threat landscape. Companies are competing against adversaries – those that are either intentionally targeting them, or just looking for open hosts to attack. To develop an effective strategy, an organization must define which assets, networks, and information are most important to defend. This then leads to a more appropriate allocation of resources – people, money, tools, etc. to those areas that are most critical to defend.

We believe the past decade's focus on "information" system risk assessments has left the most critical assets of most companies' IT infrastructure at risk – namely the control systems. My former colleagues at McKinsey recommend prioritizing a company's information assets, and then go on to describe the various types of information to protect. However, in most industrial, healthcare, logistics, transportation and other product or service companies the most critical technology assets include production and control systems, not just data storage or processing systems.

Our approach focuses on prioritizing where to compete in the operational technology landscape. Each asset or network does not pose equal risk to operational performance or information leakage. Further, each asset or network may have a different exposure to potential competitors or threats. The first step in any strategy is to define how to prioritize where to focus.

This type of strategic prioritization is not the realm of IT consultants or traditional cybersecurity analysts; it is the realm of process engineers, control system programmers, and embedded system analysts. To determine where to focus, a company must assess its processes, identifying those assets and networks that are most critical to its operational uptime, quality, delivery time or other operating metrics. To do that requires people that understand the processes and OT networks that drive these systems. We are always amazed at the number of cybersecurity consultants that try to assess threats in OT systems with people that have never been in a plant, run a process control network or optimized a supply chain system.

There are a range of tools we use to build this prioritized list. Process mapping, asset inventory to understand the age and vulnerability of each asset, network mapping to understand the connectivity between components and networks, and machine-learning based risk modeling to understand the implications of failure or compromise of different network elements.

Most critical, however, is a team that understands the underlying control systems and processes in these environments that can take that analysis and synthesize it into a set of concrete recommendations about the types of actions necessary to build a cybersecurity program.

Step 2: Target Setting

In a corporate or business unit strategy, successful practitioners would always establish targets and objectives prior to defining their action plan. So why is it in cybersecurity so many organizations can't answer the question: "what is our goal?" or "what does distinctive performance vs. average performance look like?". The fundamental problem is the fact that the threat landscape is constantly evolving and success is like proving a negative – i.e., "we've never been hacked so we must be secure".

We strongly believe that successful control system cybersecurity begins with clear, ambitious, measurable targets. To paraphrase Lewis Carroll, "If you don't know where you are going, any road will take you there." Being more secure or "best-in-class" in cybersecurity is a never-ending chase down a new path that evolves as new threats emerge.

So, how to set those targets? The great news is there are a range of standards available – from ISA, to CIS/CSC 20, to NIST, to NERC-CIP, to ISO 27001. We are not saying any of these are perfect. But we also believe in not letting perfect get in the way of the good. We work with clients to select the most appropriate standard for their situation. Then we tailor – in line with their unique operational and cultural character – to an appropriate target. Finally, we set clear, objective scoring criteria for each element. This last piece is most critical. A vague objective to "identify assets" will not drive the kind of results you want to see. Clarifying "asset identification" with items such as what types of info you want on each asset, how often that information should be updated, what assets are included or excluded, and what to do with new assets that are either approved or unapproved are all critical elements in defining a set of milestones for security controls.

But what about timing? Not all of the goals are achievable at once. And, importantly, certain objectives rely on primary steps being taken. Therefore, we lay out a maturity curve objective that builds off early steps to grow security over time. This curve should have firm, hard deadlines so teams can know what their objectives are and when those objectives need to be achieved.

Step 3: Set appropriate budgets

Once a company has established its prioritized set of where to compete and clarity on the targets of what is the security objective, it must then set budgets appropriate to achieve that strategy. So often companies do not have a measurable way to set cybersecurity budgets because there is no clear outcome to measure success against. However, the above process enables companies to have a fact-based set of potential outcomes and targets. Our model is similar to the way companies would assign maintenance budgets or controls upgrade budgets.

Perhaps most importantly, cybersecurity budgets should be integrated with operational planning cycles, not addenda to the overall budgeting process. Like safety or maintenance, cybersecurity is a fact of doing business in today's environment. Managers should be held accountable for driving business performance while maintaining security and risk management. We are not advocating that no incremental spend is required. In fact, in most cases cybersecurity has never been a consideration in controls networks, so it is additive to budgets. But we strongly believe it needs to be considered as part of the annual planning cycle so operational teams tasked with P&L's can understand their risks, the costs of reducing those risks, and help make the appropriate cost-benefit trade-offs – with the right external support and guidance from cybersecurity experts in the company as well as from the broader cybersecurity market.

For instance, when cybersecurity is factored into capital planning, device or software upgrades may make more economic sense than if only looked at as maintenance. Without these integrated set of budgets, the whole picture is missed.

Step 4: Design "How to Compete"

Again, we use the term "compete" to highlight the need to defend against real threat actors, but in this case, we focus on what set of initiatives a company should deploy to address the key risks and objectives highlighted in steps 1 & 2 above. While I was at McKinsey, the firm developed a very successful strategic framework called the "portfolio of initiatives". The concept is to lay out a set of initiatives across three horizons of time.

- Horizon 1: Initiatives that can be done quickly and achieve near-term impact.
- Horizon 2: Those that require more infrastructure or organizational change.
- Horizon 3: Finally investing some resources in initiatives that can deliver longer term, transformational impact

The term "initiative" is important in this context. An initiative should deliver an outcome, not just take an action. For instance, all too often cybersecurity programs become a series of tool deployments, training programs, and playbook generation. Many times, the outcome and goal is forgotten in the pursuit of the actions. Initiatives are a set of actions that taken together deliver an outcome. For instance, we often find that the first initiative is to build an inventory of asset vulnerabilities and risks. In some cases, companies hear "asset inventory" and immediately conclude they need a new tool to find all the assets on their network. But the initiative makes this more holistic. Perhaps a tool is necessary, but thinking through what the end result looks like - a database that is linked to vulnerabilities, managed over time, able to include manually-entered risk information, providing deep information on each asset necessary to assess its lifespan and risk, etc is the key. By considering this as an "initiative" takes away the likelihood of ending up with a stream of new tools, each of which requires new skills just to manage it.

Like most successful frameworks, it is relatively simple. But it forces you to get specific about which initiatives will deliver what benefit in how much time and at what cost. It allows you to tie initiatives to specific areas of the controls networks that are at greatest risk, and then link those to the targets set in step 2 above. Further, by breaking things down into smaller “initiatives” the budgets can be seen granularly rather than as a big bucket of “cybersecurity”. Each initiative can be budgeted and tracked at an individual level and over time the overall security maturity of your organization can also be measured, tracked and reported.

Step 5: Measure & Report

No strategy is successful without measurement and reporting that can tie back to success. As outlined in Step 3 above, a clear objective is critical to effective cybersecurity strategy. By setting those objectives and building a measurement and reporting culture and capability, senior management can then understand the initiatives that are driving improvement, those that are falling behind, and most importantly, where new initiatives need to be added to close gaps that might have been unforeseen in the initial strategy-setting. The notion is that these initiatives must iterate over time as new learnings and information emerges.

Measurement and reporting provide three critical results:

1. Measured success of the portfolio of initiatives. As we have said above, all too often cyber programs devolve into deployment of a set of tools to solve each seeming new individual threat. This is impossible for senior management to assess or measure. By breaking goals down into specific initiatives, each with a clear objective measurement, senior management now has transparency into whether initiatives are delivering the effects as intended. For instance, one company told us the story of their success in deploying backup tools in each facility. Unfortunately, they were not measuring regularly whether those backups were occurring on a regular basis or if the backups they were receiving were correct. When an incident happened, the tool had been deployed, but the actual objective of that “initiative” was not achieved when they realized that no backups actually existed. Measuring the right things and providing transparency with clear metrics is critical.
2. Determine where new or additional resources are required. All initiatives will not be equally successful. By tracking on a regular basis, management can see where certain initiatives are not achieving their desired outcomes and more or different resources are necessary. For instance, in many cases the equipment in control systems is old and many of the latest security features are not available or safely applicable. To achieve improved cyber security oftentimes these devices will need to be switched out over time. With a clear set of metrics, measures and reporting senior management can plan and track the replacement of these older systems as part of an overall program. And in cases where the pace is falling behind desired objectives can reassign resources as necessary to complete.

3. Add new initiatives/replace old where appropriate. One of the most common areas of this has occurred in protecting against malware in control systems. Most cybersecurity programs started with deployment of anti-virus solutions similar to the IT world. However, after a month or a quarter, most of the signature files of these systems become out-of-date as the operators do not want to patch running control systems. So, by measuring the true effectiveness of these anti-virus solutions with metrics on the most recent update dates, etc., management finds that an alternative solution to that initiative – i.e., application whitelisting – is critical to achieving the original objective. Without detailed reporting on dates of anti-virus updates this issue might have gone unnoticed until an incident happened.

Remember that reporting does not need to be onerous. Automated solutions to gathering such data across multiple control systems now exist to help reduce the burden and increase the effectiveness of such reporting.

Summary

Cybersecurity strategy can learn from the basics of corporate strategy development over the past half century. Control system cybersecurity strategy has been overlooked for many years as the regulations, compliance, tools, and dollars have focused on "information system" security. We believe that an appropriate cybersecurity strategy for most companies would identify control systems as a critical area where they need to compete with adversaries to protect the safe, reliable, expected operation of their facilities.

A five-step process can help ensure that a company focuses on the right assets to protect and builds a program over time that delivers measurable cybersecurity improvement linked to the operational budgets of the business.