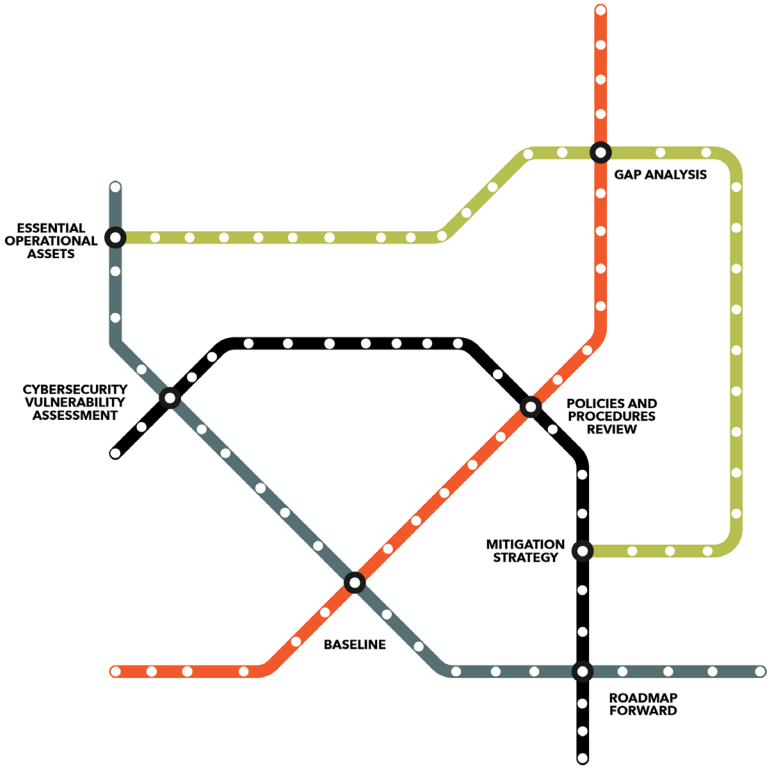
FOXGUARD SOLUTIONS®

Developing a Cyber Security Strategy and Roadmap

For large/complex transportation networks, starting on your cyber security journey can feel overwhelming, but there are simple steps organisations can take to develop a robust strategy and roadmap, writes George Ifebuzo, Sales Director at FoxGuard Solutions, a wholly owned subsidiary of Framatome.



Maintaining widespread security over vast geographical regions is no easy task for rail networks. However, it is far from impossible.

First, creating a secure digital environment can be broken down into steps, starting with determining what assets are essential to an organisation's daily operations.

Running through each business process, from how a customer buys a ticket, to how a train gets safely from point A to point B will likely highlight that your business relies on more assets and applications than initially thought and will help you redefine what's critical to daily operations.

In our experience, companies tend to focus resources on their most critical assets, which makes sense, but oftentimes don't realise the effect a peripheral system can have on operations if it becomes unavailable. We've seen attackers focus on these less protected secondary systems and still impact critical operations, so it's key to scrutinise every aspect of your operations.

The Cyber Security Vulnerability Assessment

Determining what's important to daily operations goes hand-in-hand with undertaking a cyber security vulnerability assessment (CVA),

which many of the latest security regulations require. It's a perfect place to start because this exercise walks you through examining what you have in place while opening your eyes to what's at risk.

When we perform CVAs on behalf of clients we typically start with a policy and procedure review to get a good perspective between the organisation's policy expectations and how it actually operates. This gives you a well-rounded view of your current cyber-security stance and using this information, you can establish a baseline of operations, which shows exactly how your business is currently run. This will include an inventory of assets, their configurations and the controls in place.

From here, the next step is to undertake a gap analysis, which enables you to see where security gaps exist.

For example, you might have robust policies and procedures in place, but that means nothing if staff only follow them 20% of the time. If your work culture encourages getting results over following procedures, staff may be using shortcuts that enable them to complete a task and creating unnecessary security risks. Knowledge gaps can be another issue – if training doesn't address key security procedures someone could easily turn off a device feature that was preventing a cybercriminal from taking advantage of a system vulnerability.

Developing a Mitigation Strategy

With these steps completed, you now have full view of your organisation's cyber security gaps and can begin creating a mitigation strategy.

We take a first aid approach to this: put pressure on the wound, stabilise the patient and then talk about treatment.

A mitigation strategy begins by taking the results of the gap analysis to prioritise what's the highest cyber security risk to your organisation.

Alongside this, you'll come across low-hanging fruit, quick fixes enabling you to close security gaps immediately. While they might not be the most critical issues, they're easy wins that help mitigate risk and stop the bleeding.

Having 'stabilised the patient' you can then target those larger tasks that will bring your organisation to a much more secure position.

In order for your mitigation strategy to be successful it's imperative that the technical team and leadership agree on the approach they're going to take. This is because the best way to destroy a good strategy is to not have leadership buy-in. In addition the mitigation needs to fall into the risk appetite of the company and be cost effective to move on the solution.

Good Can Be Good Enough!

The goal with this process is to remove risk because every gap that's closed – no matter how small – makes your attack surface smaller and creates a more secure environment. It's easy to get wrapped up in working towards perfection – something that's in fact unattainable as cybercriminals will always be trying to get one step ahead – so don't let perfection be the enemy of good.

Cost can also be an issue, particularly as some of the biggest security gaps can be the most expensive to fill and without a clear return on investment (RoI) attached to the work it can be tougher to get boardroom sign off.

In cases where the budget simply isn't there, look for alternative controls or solutions that will, at the very least, improve your level of security. Simply put, do the best you can with the budget you've got. Try to always talk the language of business risk when asking for resources. Oh, and remember this is a marathon, not a sprint. Few companies will be in a position to quickly fully secure their organisation, whether that's due to funds or human resources.

For example, how would you implement an antivirus for an organisation as large as Amtrak? That's 25 states, 400 locations and who knows how many devices. You can't do that overnight – this can take weeks to plan and deploy in organisations of this scale, and is just one aspect of a robust cyber security programme.

The Culmination: A Roadmap Forward

Your mitigation strategy should be developed in partnership with your roadmap forward. This brings everything together into a strategic direction that the business can get behind, having assessed its current

cyber security level and seen where the vulnerabilities lie. It also won't be the first time executives have heard or seen what is needed to improve your security.

It reflects what can be realistically accomplished, given timelines and budgets, but again requires buy-in, this time from the entire business: shopfloor staff through to the C-suite.

Not everyone may be actively involved in actioning this roadmap, but many in your organisation are likely to be affected by the changes it brings at some point. Improving cyber security will likely include work practice changes and implementing new processes and procedures that may slow things down or restrict access.

If you want to encourage a more security-minded work culture, it's important not to simply add security on top of existing process. Instead, try making secure work practices part of the way all work is done.

By doing so, you're more likely to develop a company culture that nurtures a robust, mature cyber security programme, as security shouldn't be the extra task you do at the last minute; it should be the way you perform your tasks.

Don't Make This Journey Alone

Having the right partner to guide you through these steps can simplify your cyber security journey and ensure you don't overlook potential vulnerabilities.

FoxGuard Solutions can help you break down and prioritise the steps needed to develop and maintain your cyber security programme and provide expert support along the way.

Find out more about how FoxGuard Solutions can support you by visiting our website **foxguardsolutions.com/transportation-rail**.

Where to start

1. Determine what's important to operations
2. Undertake a cyber security vulnerability assessment (CVA)
3. Carry out a comprehensive review of policies and procedures
4. Establish a baseline of operations
5. Complete a gap analysis
6. Develop your mitigation strategy
7. Create your roadmap forward

George Ifebuzo

Director of Sales

gifebuzo@foxguardsolutions.com

+1 704 330 3521