Security elasticity. A holistic approach to incident response.

Building a layered incident response strategy

The global energy system is increasingly relying on digital technology to meet growing demands for efficiency, but along with the rewards come a myriad of challenges. The same digital innovations that ensure that the energy networks are fully optimized and managed efficiently make it more vulnerable to external attack.

For energy systems to operate safely and reliably, this threat must be understood and protected against for both new installations and the vast legacy network that is currently deployed.
A recent incident occurred in March 2019 when a major production facility in Northern Europe had to revert to manual operations following a ransomware attack known as LockerGoga. During the event, facilities around the world were unable to connect to the company's production systems. The growing frequency of such breaches is being driven in large part by the steady increase in connectivity of industrial systems. This increases the challenges faced by enterprises as they struggle to keep up with this trend by rolling out new cybersecurity measures. These attacks highlight the importance of a strong cybersecurity strategy that covers the entire cycle from prevention with a robust cybersecurity baseline, through to incident response driven by training drills, and from appropriate playbooks to recovery and effective communications. At the heart of this are people, process and technology that form the backbone of ABB's cybersecurity portfolio.

The steps to develop an effective defense.

In today’s energy landscape, it is important to design a cybersecurity program with scalable and adaptive incident response. Cyber resiliency needs to line up exactly with an organization’s enterprise risk management principles, so that the teams are exhibiting what we call security elasticity.

When an incident is detected

A response life cycle can be broken down into four phases, from the first occurrence to customer notification

We look at these common time metrics to measure an organization's ability to respond to a security incident. While we want to shorten every phase of an incident, this paper will focus on one that your organization has direct control over - the discovery to containment period. After a cybersecurity incident is detected, every passing moment is critical. What you do in this period impacts what you do in the investigation and notification phases later. How well an effective plan can be swiftly deployed determines the severity of the damage.

Actions taken can impact:

- Your ability to get back online
- Your customer experiences
- Your reputation, and
- Your bottom line in the form of fines

Who to engage?

The first step to building security elasticity is building the right team. In order to avoid redundancy and reduce complexity, it is important to include only the most necessary players needed to respond to, and remediate, an incident.

If you are relying solely on your security team to get the job done, think again. Engage those internal stakeholders outside of your immediate security team that can give your team the air coverage or the buy-in needed to run the incident response.

Assigning a strategic team comprised of leaders from security, risk and operations works best, so be sure to include executive stakeholders, such as your CRO or COO. From an operations perspective, including these stakeholders ensures you have buy-in on procedures, and you have boots on the ground to implement alternate controls, containment or changes in operations to get back online.

For risk, it ensures alignment to corporate risk thresholds and strategic priorities. You need the enterprise risk team not only to help the security team align to corporate priorities, but also to accurately assess impact and likelihood of risk.

Next, you will need to activate your functional stakeholders, such as communications, legal, operations and customer support. Communications will facilitate holding statements, protocols and crisis communication while legal addresses client-attorney privilege policies and disclosure obligations to parties such as law enforcement or contractual partners. Additionally, operations can focus on remediation, recovery and forensic data as your customer support stakeholders dial in on proactive advisory and general support.

And let us not forget about your suppliers. Industry leaders are now taking a proactive approach to incident response by leveraging supplier capabilities. For instance, you can regularly engage suppliers in incident response drills. They can be used to confirm your incident response team and processes, or they may create proactive scoping documents to facilitate faster recovery.

So, what is the lesson here? Connect your entire team and stakeholders now; not later. Building the right team builds trust, and trust builds security elasticity. Having the right internal and external stakeholders in the room instils confidence and ownership, reduces redundancy and improves reaction times.

How to implement the fix

This brings us to step two. Once you have the right team in place, it is time to effectively implement your plans.

There is a growing skills gap in cybersecurity that may be directly attributed to an over-reliance on checklists and policies. Think of it like a playbook on a sports team. It is great to have go-to moves, but if that is all you have in your arsenal, there is little room for creativity.

Playbooks are often too tactical. They consist of a re-assembled set of tasks triggered by the detection of a threat. This can delay your teams in reactive, tactical checklists and steps, instead of placing more effort on strategic, proactive measures that can help prevent attacks. They are simply not dynamic enough to allow your team to grow.

So, remember these three words: drill, drill, drill. If you want to build elasticity into your processes, run highly realistic drills. Running various drills promotes the creativity needed to build your security elasticity. Drills help you account for the myriad of scenarios you may face and can help you understand where you might improve. But most importantly, they build a culture of adaptability that will help you to work well under pressure and identify efficient solutions for continuous improvement.

What is the lesson here? Do not rely solely on reactive check lists and policies to prepare your teams for an incident. Build elasticity into your processes by running highly realistic drills that reflect your risks and your environment.
This instils confidence and builds a culture of creativity.

How to get better

Once you have successfully implemented your plan, it is time to reflect. By nature, incident response teams are under high scrutiny from leadership. It is important to build a culture of continuous improvement by recognizing successes and workshopping failures. Do not underestimate the power of a post-project discussion.

Being able to qualitatively track how your team has performed, as well as being able to track results qualitatively, is critical. Plan from the beginning to instil into your processes the acquisition of evidence to show your progress. Get used to talking with your teams about what could be improved and what needs to change moving forward.

Second, measure how your teams are trending to see your improvements and where you can invest to get better. Looking back at our incident response life cycle, ask yourself two questions:

- What kind of trends do I recognize?
- Have I made enough investments to strengthen my team’s weaknesses?

Building the right team and instilling it with creativity through realistic drills will significantly reduce your times across every phase, particularly in the time to discovery.

The lesson here? Document the metrics that matter and continuously measure to improve your progress. By capturing what you did and what you could do better, you are building a continuous improvement loop for people, process and technology where it is safe to point out what could be done better, what was done well and have the flexibility to make the right adjustments.
This will ensure security elasticity.

Do not wait until an incident to learn about incident response. To stay prepared, it is vital to build security elasticity into your organization. To do that, you must understand and define your internal and external partnerships to build a well-organized team; instil response creativity in your teams with highly realistic drills; and measure what matters for continuous improvement.

ABB Proposition

In its simplest terms, cybersecurity is all about people, process and technology. ABB has the domain knowledge and experience in the energy sector for automation and control technology. We bring our rich heritage and deep understanding of the industry and the challenges that it faces. At ABB, we have an installed base of more than 70 million connected devices, 70,000 digital control systems, and 6,000 enterprise software solutions.

As a leader in the industrial space, we have four decades of experience creating secure digital solutions for customers in critical business segments, such as oil and gas, power generation, and distribution. We provide the defense-in-depth security that is a prerequisite for modern energy companies. Over the years, cybersecurity has become an integral part of ABB's product portfolio. Today, it is front and center at every phase, from design and development to product maintenance and support.

—

ABB
Operating in more than 100 countries

abb.com/cybersecurity