Securing critical infrastructure

verizon

About the author

Doron Harel is a cybersecurity professional with more than 30 years of cross-functional experience across a wide range of industries. His cybersecurity experience spans disciplines including Enterprise Security Architecture, Risk Management, Information Security Governance, Audit, Compliance, Cloud, and Fraud. His strong technical leadership, coupled with his business acumen, helps Doron solve complex client challenges and present solutions in an understandable business context.

Doron Harel
Head of Cyber Defence
Verizon

Contents

01 Introduction

Introduction

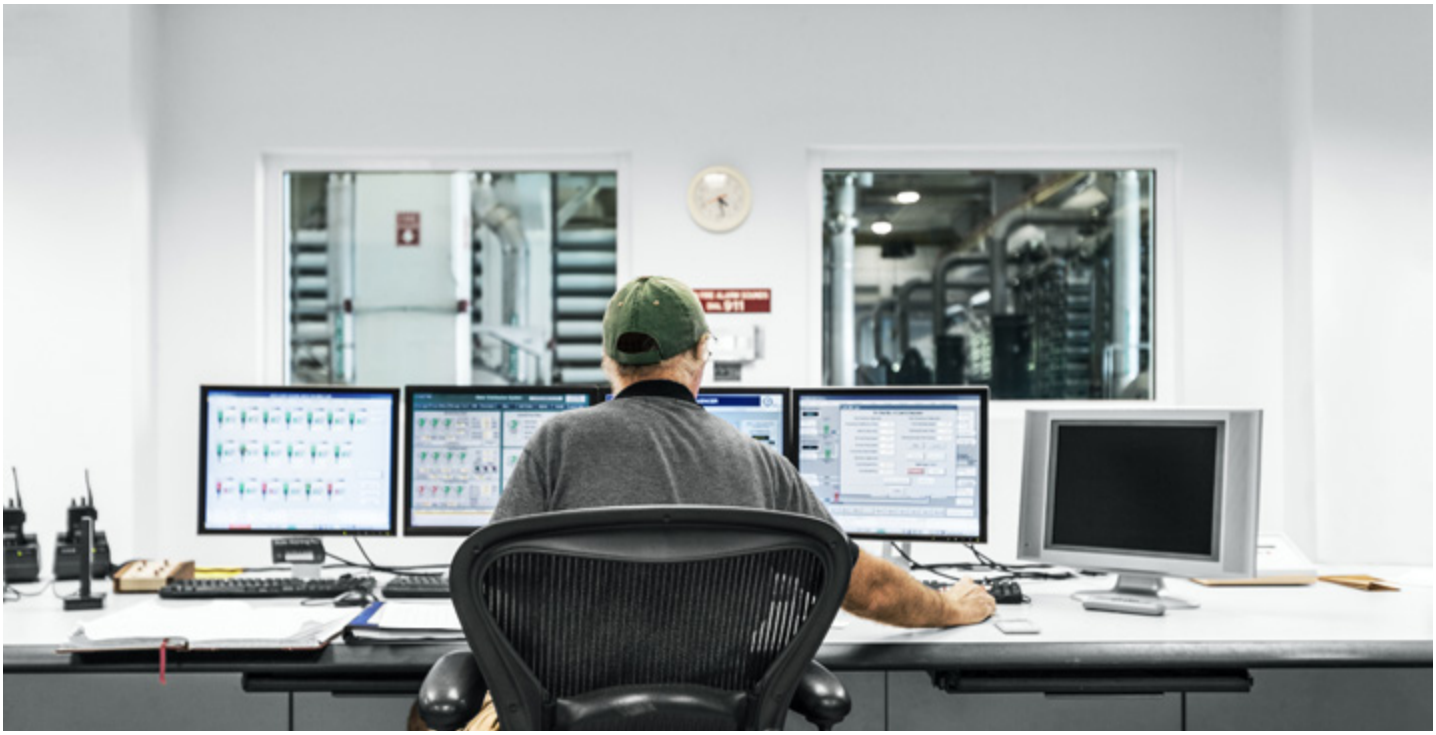
Governments are having to work out how to protect their critical assets. Some assets are managed by themselves, and some by the private sector, but all fall under the state's responsibility to provide services and protect its citizens. Which is why we have seen governments in recent years developing and enforcing security regulation over critical infrastructure.

A critical infrastructure sector can be described as one whose assets, systems, and networks, whether physical or virtual, are considered so vital to their country that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

As more critical infrastructure is digitalised to respond to the increasing needs of society, the attack surface increases – and with it, the prospect of life-threatening disruption. This is a conundrum that is further exacerbated by the fact that Operations Technology (OT) often exists outside of Information Technology (IT), with one being more concerned about productivity and efficiency, versus the other whose priority is cybersecurity.

Organisations understand the price of not complying with current regulations, but the cybersecurity impact can be even greater if an organisation is hit by hacking activity, ransomware, or stealing their "Crown Jewels".

Ransomware attacks have targeted everything from private businesses to the government to hospitals and health care systems. The latter are especially attractive targets, given how urgent it is to get their systems back up as soon as possible.



“For every new piece of technology that we introduce into an organization, we add a new attack vector that requires protection.”

Jeff Schwartz
Vice president of US Engineering at Check Point

One such example of a cyberattack on a critical infrastructure was the attack on the Colonial Pipeline, which supplies about half of the East Coast of America’s gasoline. It was the victim of a cybersecurity attack that involved ransomware, forcing the company to take some systems offline and disabling the pipeline for several days, causing gas panic-buying, shortages, and price spikes in some states.

About a month after the attack, it was found the likely breach was through a leaked password to an old account that had access to the VPN and was used to remotely access the company’s servers. The account reportedly didn’t have multifactor authentication, so the hackers only needed to know the username and the password to gain access to the largest petroleum pipeline in the country and since Zero-Trust wasn’t set up either, it meant everything could be accessed, not just one designated piece.

This is one of the reasons that cybersecurity is now at the top of the agenda for most critical infrastructure organisations.

There are already generic and industry-specific frameworks that organisations can choose from or must follow, like NIST CSF, 800-xxx, COBIT, NERC, NEI, ACSC’s Essential 8, AEMO’s AESCSF, ISO 27xxx and many more, but it’s hoped that the latest developments in legislation will help improve national cyber resiliency still further.

02 Australian regulatory developments

Australian regulatory developments

As the vulnerability of critical infrastructure to cyberattacks has become more widely recognised, the government has increased its efforts to help protect the Australian economy and society as a whole.

Timeline of government initiatives

2017

Australian Government creates its Critical Infrastructure Centre (CIC).

2018

Introduction of regulatory frameworks through the Security of Critical Infrastructure Act.

2020

The government works with industry to develop the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill).

2021

Australian Government expands legislation to more industries.

Before and after

The government now plans to expand the existing legislation to cover more industries and sectors and increase the liability for relevant organisations.

Previous legislation covered

- Education
- Food
- Transportation
- Energy

The new legislation covers

- Communications
- Financial services
- Data storage or processing
- Defence industry
- Higher education and research
- Energy
- Food and grocery
- Healthcare and medical
- Space technology
- Transport
- Water and sewerage

While we can look at each vertical separately, some of the challenges and security risks are the same. From a cybersecurity view, this makes it easier to manage and mitigate. After all, using the same set of architecture, processes and tools makes the security less complicated and reduces the chance of mistakes.

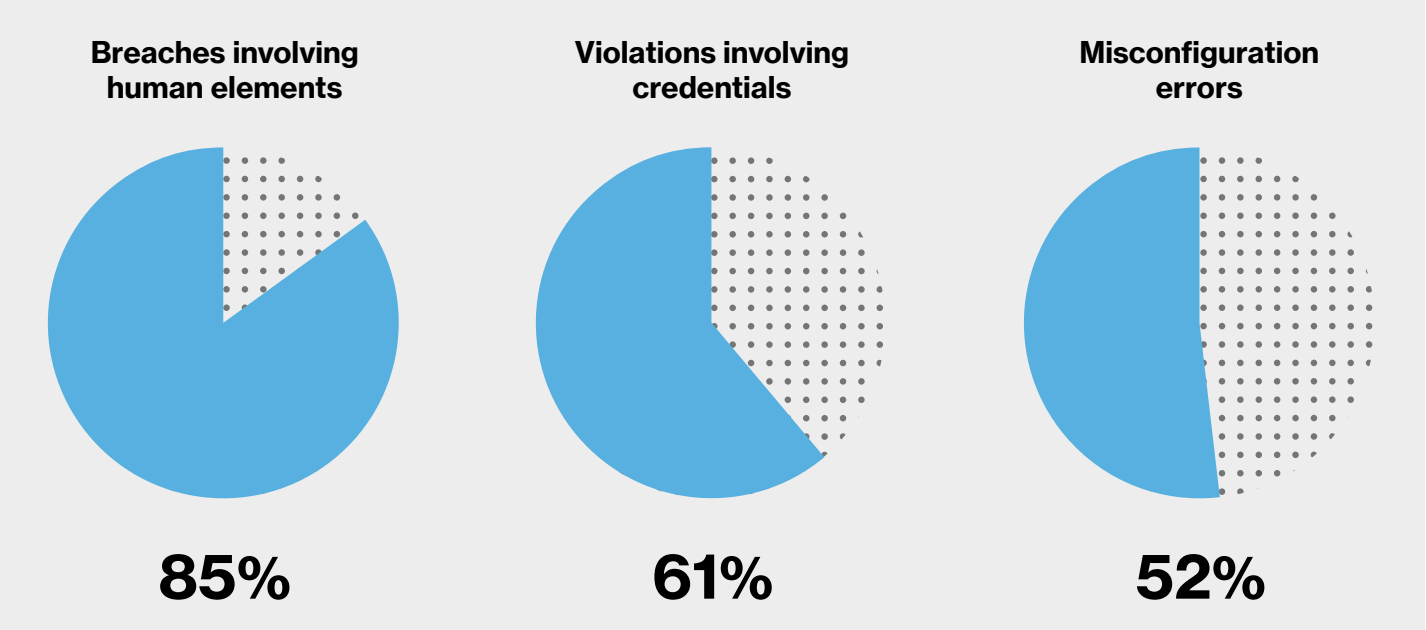
Security threats and responses must be understood in context. In Australia for example, while global frameworks such as ISO27001, NIST or COBIT may be applied, specific local standards apply, such as the ASD Information Security Manual or IRAP certifications for protected data.

03 The human challenge

The human challenge

The human factor has a significant impact on cybersecurity. A lot of the controls aim to protect the system from human mistakes. While most security experts agree that 'humans cannot be patched,' it's more than a phrase. According to Verizon Data Breach Investigations Report (DBIR), some of the key findings from the 2021 report reveal that 85% of the breaches involved human elements and 61% of the violations involved credentials. And it's not just end users or admin that make mistakes, security admin does too, because making miscellaneous errors is just part of being human. DBIR data shows 52% of the errors were misconfigurations. We can assume some of this was on security tools. There is a way to reduce this by implementing a Security Orchestration, Automation and Response (SOAR) solution.

The same applies to people working with the Operations Technology. Like all other users, they work under a lot of pressure, and this can increase the chance of mistakes. The hackers know that and are constantly trying to find a mistake they can leverage.



Some of the key findings from the 2021 DBIR report

Security isn't something you claim, it's something you prove. Best practice sovereign teams will be able to document vetting standards such as NV1 and certifications including VTRAC, CISSP, CISM, CISA, CRISC, CSK, SABSA, TOGAF, ITIL and COBIT.

04 IT/OT networks, a new era?

"The hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events."

Operational Technology (OT) as defined by Gartner

IT/OT networks, a new era?

Just the mention of OT security can cause a security expert's body to chill, and with good reason. Flat legacy networks can have 'weird' protocols that IT technology cannot understand, build, or maintain. While there are many regulations and frameworks to follow, they are not always strictly enforced.

The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems (ICS) environment.

OT security is practices and technologies used to:
(a) Protect people, assets, and information.
(b) Monitor and/or control physical devices, processes, and events.
(c) Initiate state changes to enterprise OT systems.

What makes the OT environment unique is the potential impact of a successful attack. The damage to critical infrastructure could be much worse than the effect of financial or health information disclosure – lives are at risk. How many are willing to live without running water for weeks? Or tolerate loss of electrical power for days and weeks? If an organisation is hacked or bridged just once, we all feel the outcome.

And it's not just cybercriminals we need to worry about. The new emerging threat is from hackers' groups operating on behalf of foreign governments. Their aim is not just money or just because it's possible. Successful attacks can cause a domino effect impacting many other industries, perhaps even a whole economy. Their targeting of utilities and energy organisations is a weapon in a foreign power's arsenal as part of a war happening in a new dimension. State sponsored attacks are sophisticated and tailored to hit specific organisations. They have unlimited resources and the time to prepare an attack and bypass security controls.

Timeline of major hacks

With an average of 200 days before malicious activities are detected, we can only assume that there are always uninvited guests inside the network.

These cyberattacks emphasise the need for governments to improve regulations and enforcement to protect our privacy and our way of living.

But can we hold organisations accountable for breaches, when even the security vendors (their products, and the companies themselves) are compromised? Looking at the impact of the SolarWinds vulnerability, this was a global, cross-vertical event, affecting everything from mid-sized financial organisations to enterprise and US government agencies. SolarWinds is not the only one – take FireEye and Palo Alto for example – the threat is real and ongoing.

Security solutions need to be handled by security professionals, because network infrastructure and security are complex areas requiring special skills to build and define end-to-end solutions.

So what can organisations do? Global standards and regulations cannot provide an "off the shelf" solution. Each network is unique (even if using the same technology). A tailored solution is required that considers many variants.

When talking about OT, it is important to extend the conversation. An IT approach can have a significant impact on the OT side. Not as another layer, more about the way it takes account of the relationship between people, process, technology, and culture. All are important for resiliency to cyberattacks.

Are Zero Trust and SASE part of your OT or IT transformation initiatives?

Only a few organisations maintain a separated OT environment. Most of them use shared resources between IT and OT. This saves money, but what about the security risks? When looking at the combination of the two, there is a need to consider all the new IT initiatives like cloud transformation, the adaptation of Zero Trust and SASE frameworks. There is no doubt that OT needs to be part of this design. Using cloud services can provide significant value to organisations and the development of the OT. For example, using smart meters that report to the cloud, or using API gateways for some other services. Typically, these projects develop in isolation, with no real integration between IT and OT, other than maybe on the edges. To be protected, both IT and OT need to share information about threats and risks.

05 CISO challenges

CISO challenges

There are common business challenges: lack of visibility, securing the convergence of IT/OT and cloud and, of course, improving OT security whilst maintaining availability and up-time. To deal with the security challenges, organisations have a role and function that is responsible: the CISO. While the CEO is ultimately accountable for the company's security, the CISO is the role that deals with this directly. The CISO is responsible for the organisation security, both IT and OT.

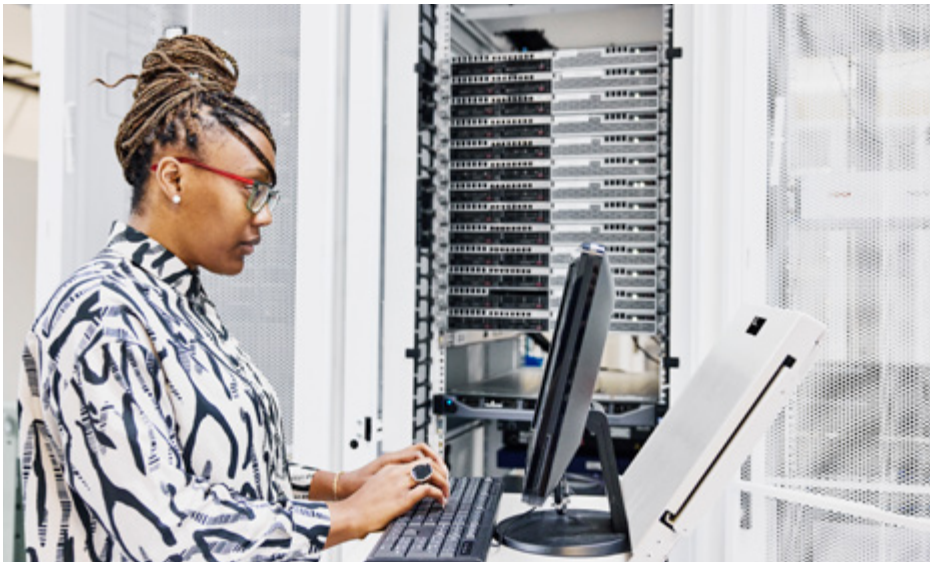
Organisational structures and technical challenges can result in CISOs having limited control over the OT

Internal politics can also affect the ability of the CISO to own the security posture. The operation leaders influence the wider leadership team. After all, they are the revenue generators on the business side, while security is just a cost centre. The organisation's hierarchy also plays a part. Who does the CISO report to? To senior management, or outside the typical hierarchical structure? This can be an indication of how seriously the organisation takes security.

The CISO role has also started to evolve beyond just Security Officer. The role requires developing business management, relationship management, and other soft skills to be successful. In effect, the CISO becomes CBSO – Chief Business Security Officer.

On the technical side, OT security controls are usually separated from IT. Even if the same security tools are used, it might be on a separate console because the OT selection criteria are different than for IT. It's more difficult to share information or threat intel when security teams are separated.

Cybersecurity is not, and should not, be treated as an IT issue only. Security affects every aspect of an organisation. It is no longer just something the IT staff can handle on their own. OT environments are not more complex than IT, just different. Comparing standard IT systems with OT systems such as programmable logic controllers (PLCs), RTU, supervisory control and data acquisition (SCADA), and MES (Manufacturing Execution Systems) devices and systems used on manufacturing plant floors, IT systems tend to follow the Confidentiality, Integrity, and Availability (CIA) Triad, where confidentiality comes before everything else, while OT systems follow the AIC Triad, where availability is prioritised overall, and integrity is valued over confidentiality.



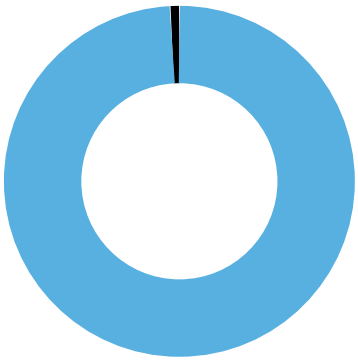
“The challenge is not with technology. If it was the case, then it would be an easy fix. The real challenge is to change the mindset of other stakeholders.”

It’s hard work, and takes time and effort, but the reward is a company ready to face future challenges.

Compliance with regulations and laws is not the end game. It’s the first and essential step in a long journey. In the crawl-walk-run stage approach, most organisations are at the “crawl” phase, even if they think they are in the “fly” stage. Like many other journeys, the first step is the toughest. To face reality and look at the organisation as a whole and understand that now is the time to start. Organisational security is more than just deploying controls. It is looking inside the organisation at people, processes, and technology, and then considering the outside view of the supporting functions, contractors, supply chains and service providers. According to the Verizon DBIR report, 98% of threat actors are external. So that’s low risk for an OT “Edward Snowden,” but looking into the data, we see that 94% of data compromised was related to credentials. What we can learn from this is that hackers can find an easy way into the network, including the OT network, by compromising the credentials of internal users or someone in the supply chain.

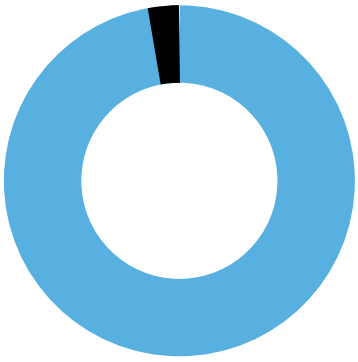
25%

Cases of threat actors being external

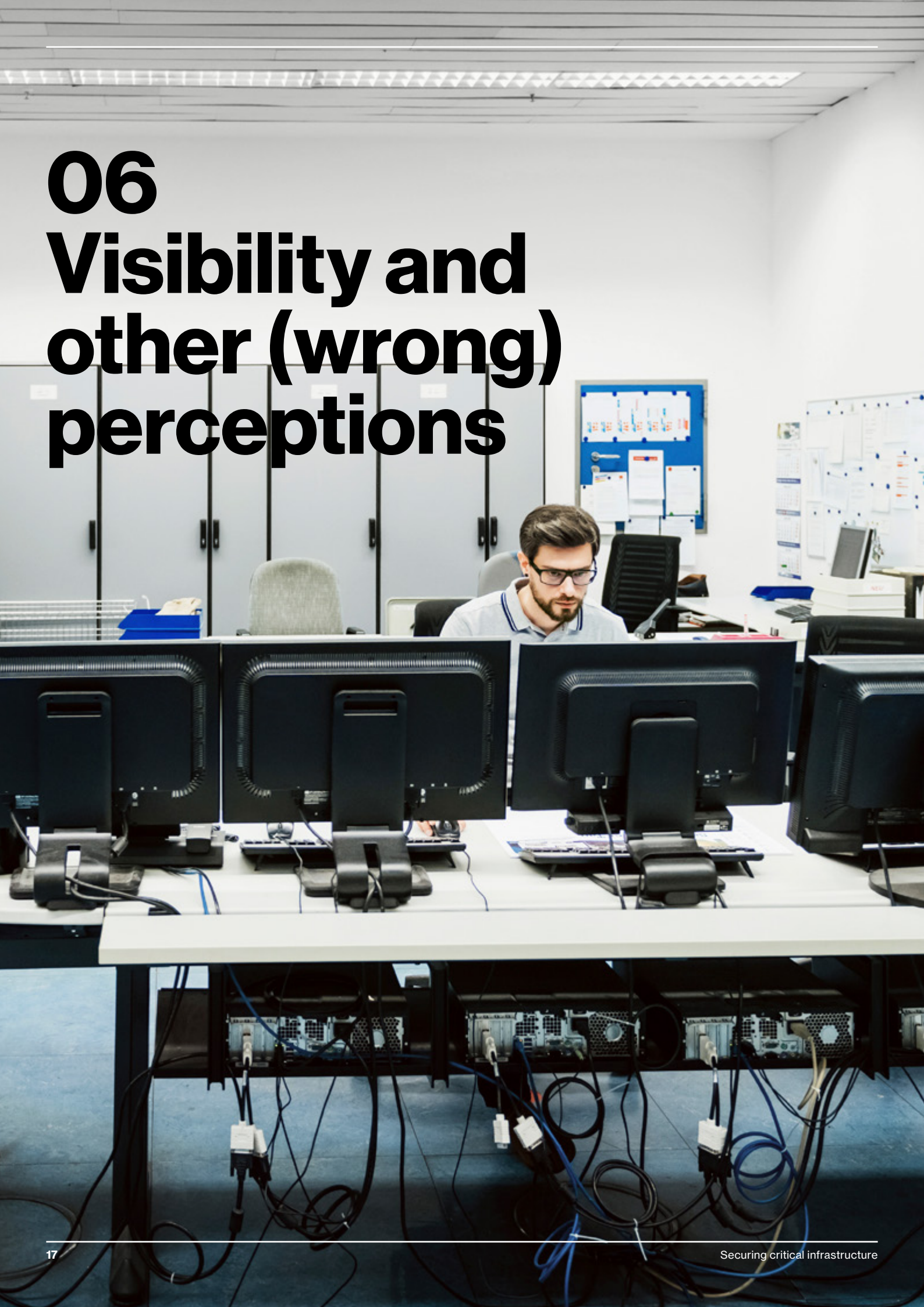


94%

Data compromises related to credentials



06 Visibility and other (wrong) perceptions



Visibility and other (wrong) perceptions

The first step with visibility is OT assessment. The initial phase of the assessment is the interview. Almost every time, there are declarations like "we are quite secure," "we have firewalls/ Access control/VM," "we mature as we have a programme, and we are monitoring the risks," and more. The detailed review of people, processes, technology and culture provides another view. Usually that they don't know what they have in their network: the number of devices, the level of vulnerability across all assets, endpoints and infrastructure, missing support for critical components, security controls not updated, misconfigurations policies and permissive rules.

And the list goes on and on.
It's only when they see that their OT environment is less isolated and protected than they thought that they can imagine what an evil "guest" can do. These are clever people – experts in their field – and yet sometimes the threat is inconceivable to them. It may be only a potential threat with a small chance of happening, but one that cannot be ignored. As they are not security experts, they believe that having tools in place is enough, without understanding the effectiveness or coverage of the controls. No one thought a Security SOC, and proper investigation function was required, or a CSIRT function should be included in the response and recovery effort. Or that OT processes ever faced actual cyberattacks.

Why is a SOC important?

A Security Operations Centre comprises the three building blocks for managing and enhancing an organisation's security posture: people, processes, and technology. It is crucial to protecting your organisation.

Cyberattacks triggered over

7,000

breaches in 2019, exposing

15.1B

records[1]

$5.04M

for those without zero trust deployed[2]

It takes an average of

287 days

to identify and contain a breach[3]

89%

of organizations rate the SOC as anywhere from important to essential to their cybersecurity strategy[4]

[1] Source: RiskBased Security.com – 2019 Year End Report Data Breach QuickView
[2] Source: IBM 2021 Cost of a Data Breach Report
[3] Source: IBM 2021 Cost of a Data Breach Report
[4] Source: 2021 Devo SOC Performance Report

07 Planning ahead

Planning ahead

When we are looking at security, we need to prepare for the future, not protect against previous attacks. The basic idea of security is to keep it simple with a defensible security posture. While there is no way to achieve absolute security, we can aim for a posture that can be defended even when it's infiltrated.

Some OT leaders are still stuck in the last millennium. A prevention approach, with a solid shell that no one can break into, is no longer valid. There is a need to focus on an actionable, pervasive model that addresses real cyber threats. Spending time, effort and money on the latest tech might not help an overall security posture, whereas a shift from "best of breed" to "best of solution" provides integration and a clear network view. Separating the product from capabilities and focusing on the outcome can help reduce the number of dashboards and screens you need to monitor, and the number of steps it takes to find the root cause.

Public stakeholders must also work with best-practice frameworks such as Federal Digital Transformation Agency, Digital Cloud and Telecommunications marketplace certifications, multi-agency HAIGS/CAGE/GovLink environments certifications or state panels such as NSW Gov. ProcureIT and Vic Gov. - ESA.

According to Verizon's DBIR Report, businesses are under continuous attack, and these attacks are getting more sophisticated and more frequent. 2 billion more attacks year on year, and somewhere around 14 billion annually. This means that no-one can take the security of their organisation for granted. It may be secure today, but there's no guarantee it will be next week, next month or next year. Wherever humans are involved, they will make mistakes and there will be others waiting to take advantage of that.

Common reasons for failures of protection

- Hyper focus on prevention of specific known threats
- "Best of breed" designs tend to focus on specific threats and tools to protect against them, not on integration or an overall solution
- The bottom-up design approach focuses on products and features
- Projects running in isolation
- Success criteria, objectives and business outcomes are often overlooked

"We should all ask where the puck will be, not where it has been."

Wayne Gretzky
ice hockey player

Vendors are developing attractive solutions to help CISOs protect their environment. They are trying to extend their solutions to cover OT too. Some vendors are offering a single solution that provides everything the CISO needs for visibility, protection, response and recovery. Unfortunately, there is no such thing as a “silver bullet” that meets all needs. The sign of a good security approach is finding the right balance between products that might not be best of breed, but ones that can work well together.

This is precisely the regulator’s intention. The carrot for a CISO is a framework that they can work with. The stick is the regulation that forces an organisation’s leadership team to provide the necessary support and comply with CISO requests.

08 Summary

Summary

The role of cybersecurity is to enable the secure implementation and execution on all assets, OT and IT, in support of the organisational strategy.

Sometimes security experts tend to forget the role of cybersecurity. The business is not built to be secure; it was created to provide services securely. Cybersecurity is an enabler for businesses to grow and develop, to explore new ways to make a profit.

To get the best outcome, the CISO needs to work with internal stakeholders, joining forces, resources and knowledge, to drive the organisation forward.

Here are some back-to-basics steps that form part of a blueprint for success.

General

- Understand the regulations and legislation
- Consult with experts to develop an actionable road map
- Develop an Enterprise architecture for IT and OT as one
- Consolidate IT and OT tools and services
- Define roles and responsibility

Technical

- **Automate** – fewer mouse clicks, focus where it counts, implement SOAR and DevSecOps.
- **Inventory** – understand what the assets are and their status.
- **Segmentation** – Adopt the Purdue model. Separate and segment the Supervisory (SCADA), Process control (PLC, RTU), Site control, and other non-production segments.
- **IAM** – Identify and centralise credentials, get complete control of who is accessing the network and hold them accountable. Check and remove any bypasses.
- **Monitoring** – Use centralised SIEM, with 24x7 security monitoring. Some PLU and RTU send their configuration as part of the log, ensuring some data is masked and anonymised.
- **Updates and Patching** – Develop update and patch program. For applications running on the old OS and cannot be upgraded, use the compensation approach.
- **Non-IP protocols** – Use specific tools that monitor and understand the protocols, even in a non-intrusive way.

Download the Verizon DBIR report here ›

For more information on cybersecurity

verizon.com/business/en-au/solutions/secure-your-business/

Sources

Engagement on critical infrastructure reforms (public)

homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-our-critical-infrastructure-reforms-engagement

AEMO (public)

aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

verizon