Taking Control of your Cyber Resilience

Digital Intelligence

BAE SYSTEMS

Building cyber resilient critical infrastructure

In July, an error in an automatic software deployment crashed over eight million Windows systems. Around the world, systems critical to healthcare, finance, and transport infrastructure ground to a halt. A fix was available relatively quickly, but many essential services were out of action for hours - and some were disrupted for much longer.

In the UK, the incident knocked out healthcare systems used by GPs. Many shops were unable to take payments. Elsewhere, travellers' details could not be processed, grounding planes; in some locations commuters could not buy train tickets. Globally, insurers estimate that the incident could cost US Fortune 500 companies $5.4bn. The overall financial fallout could be two or three times higher still. Contrast this with the WannaCry ransomware attack of 2017, which affected a few hundred thousand devices globally and is estimated to have cost $4bn in damage, and the magnitude of the error is clear.

The nature, speed and scale of the incident served as a sobering reminder of how even secure systems can be brought down; the fragility of services we depend upon for vital everyday services – critical infrastructure – and how rapidly they can fail. And how costly it can be to recover them quickly.

While this incident was not a deliberate cyber-attack, significant malicious attacks disrupting critical infrastructure have become commonplace. Since 2010, attacks disrupting government agencies and ministries, energy and water firms, healthcare providers, aviation, and telecommunications sectors have mushroomed. According to a recent survey[1] of critical infrastructure organisations, the majority of those polled said they experienced an increase in attacks - with ransomware one of the fastest growing types of threat. We've also seen tit-for-tat cyber-attacks on vital infrastructure become commonplace amidst international conflicts.

Additionally, earlier this year Western governments warned of the potentially 'devastating blow' posed by infiltration of critical infrastructure – assessed to be pre-positioning for potential attacks that could cause physical disruption to operational assets.[2]

Critical infrastructure is a high value global target for threat actors of all persuasions. It has never been more important to take active control of your resilience.

This paper considers the threat facing critical infrastructure internationally, the role of the state in creating a security-focused operating environment, and the central responsibility of business to drive improvements in cyber resilience.

The threat to critical infrastructure

Regardless of who operates them or where, critical infrastructure organisations operate in an unpredictable, multi-polar international environment, subject to both conflicting geopolitical interests and criminal forces. Critical infrastructure represents a high value target. Successful attacks offer high rewards politically and financially, and pose real threats to national security.

Attackers benefit from a thriving criminal marketplace with easy access to increasingly sophisticated and damaging ransomware, the enduring complexity of attributing attacks reliably, and jurisdictional challenges that limit the risk of punishment. The challenges of operating securely in this environment are significant. Managing vulnerabilities across sprawling enterprises is complex – particularly as threats can outpace government and business capacity to invest in the latest defensive technologies required to achieve security advantage. achieve security advantage.

The risk of disruption is influenced by multiple factors:

- **The capability, pace and impact of threats:** Cyber threats continue to advance. Threats like ransomware-as-a-service, phishing, and nation-state attacks against critical infrastructure and commercial enterprises are increasingly sophisticated, common, and capable of rapidly disrupting essential services. 2023 was one of the worst years for ransomware attacks. The general trend seen over the last few years of decreased time to exploit disclosed vulnerabilities and threat actors' abilities to unearth and use zero-days are particularly concerning for operators of complex infrastructure, who might be unable to patch quickly enough.

- **The drive for greater connectivity:** The convergence of Information Technology and Operational Technology, coupled with the Internet of Things, offers huge advantages to user convenience and remote support, for example. But greater connectivity and the associated operational complexity this can bring exposes systems to a wider range of threats, new vulnerabilities and opportunities for disruptive attacks – particularly as operational technology systems were rarely designed with cyber security in mind.

- **The technology burden:** Many critical infrastructure systems rely on technology designed to have a long lifetime. With key availability and safety factors vying with security for priority, not to mention challenges of technical debt, this can create environments that are difficult to manage – let alone secure and integrated with modern cyber security measures.

- **The cost of resilience:** Limited budgets and a shortage of skilled cyber security professionals hinder efforts to enhance cyber resilience, which can be felt acutely at both a business and national level as some sectors and countries are unable to hire or retain people with the skills they need.

- **The lack of business continuity and disaster recovery (BCDR):** When businesses lack robust BCDR plans they are more vulnerable to unexpected disruptions, whether malicious attacks or software glitches. Without a comprehensive and practiced BCDR strategy, organisations struggle to restore operations quickly. This can result in significant financial losses, operational downtime and reputational damage.

Though government and businesses face competing priorities at times, given these challenges investing in cyber resilience is critical at both a national and commercial level – underpinning national security, social and economic wellbeing, and long-term prosperity.

The role of government

Clearly governments have a fundament role to play in creating the right environment for resilience through the combination of directive and supportive measures.

The foundations start with regulations, standards and proactive guidance

Governments define what should be protected, the penalties for not doing so, and establish the machinery to monitor, guide, and help protect critical national infrastructure. There are a number of ways to create resilient cultures that hold to account both those who operate and those who seek to harm essential services. This includes: political agreements (such the UN cyber norms), international regulation (like the European Union's Network and Information Security directive 2); and domestic legislation (such as the US Executive Order 14028 on Improving the Nation's Cybersecurity, or those defining security and establishing national cyber security authorities as both technical authorities and regulators as in Jordan or Ghana).

Additionally, governments need to incentivise collaboration

Resilience across sectors and economies is not about standing alone, but comes from industry, governments and international partners working together. Alerts and advisories from national cyber security centres are essential to ensure operators are risk informed - not risk averse.

Beyond this, governments can help build cyber security workforces

Governments can play a key role in supporting the long-term development of cyber skills, training and career pathways to provide the pipeline of skilled workers that companies need. Adoption of workforce frameworks for cyber security, such as the US National Initiative for Cybersecurity Education, can provide comprehensive and consistent avenues that take students from the classroom to the work place.

Funding and incentives

Providing financial support and incentives for businesses to invest in resilience measures can encourage them to prioritise continuity planning. This can include grants, tax breaks or subsidies for implementing advanced security systems and infrastructure.

While state-level action is imperative, legislation and regulation do not deter attackers. Skills take years to develop. And incentives cannot compel collaboration or investment. Governments have vital roles in advising, enabling and encouraging organisations to boost their defences. But ultimately, organisations have a responsibility to protect themselves, their services and their users. This is particularly true if they are designated part of a country's critical infrastructure. So what can organisations do to help themselves? To understand resilience – the ability to maintain the availability, confidentiality and integrity of essential services – let's look at that incident from the summer of 2024 again.

What made some organisations more resilient than others? Many organisations were able to continue operating by being better prepared for this sort of disruption. Shops that accepted cash as well as card payments stayed open, for example. Others were just lucky as their systems came online after the error was corrected or they relied on Mac and Linux hosts. So building in redundancy and being lucky clearly matter, but aren't in themselves policies that can be relied upon or presented for board-level approval.

We can learn more by looking at how organisations affected by significant cyber incidents are able to bounce back faster than their peers. Of course, there are no quick fixes. Instead, the ability to get back online quickly stems from a commitment to building resilience into everything that matters to your core services. But where to begin?

The road to cyber resilience

Socrates reportedly said "to know oneself is the beginning of wisdom". Apply this to cyber security and it's clear that to be resilient an organisation must understand the key variables of operational resilience and how to protect them. This is not just about maintaining an up to date register of assets and systems – though that's a fundamental step. It's about knowing what the lifeblood of your business and supply chain depends upon and what could stop you providing your most essential services to customers. Understand this and you'll know what to protect, what to monitor, where to build redundancy, what to plan for and what to recover first should the worst happen.

Socrates doesn't offer much practical guidance when it comes to cyber resilience. But in our experience, the following measures make a big difference:

Commit to dynamic collaboration

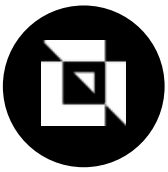
Building and participating in a trusted ecosystem that proactively and regularly shares information about threats, mitigations, and best practice will drive systemic resilience before as well as after incidents occur. The UK's Financial Services Cyber Collaboration Centre provides a leading edge illustration of how industry can develop trust in sharing for the benefit of the sector as a whole.

Adopt best practice

A recent study shows a healthy correlation between compliance and reduced breaches[3] - indicating that adopting and keeping up with the latest standards such as ISO and NIST pays dividends.

Embrace security by design

Human error remains the key threat to cyber resilience, with careless users reportedly responsible for 70% of sensitive information losses worldwide last year.[4] However, while training and education are of course vital, they cannot eliminate mistakes and accidents. Instead, better design is the key to reducing the likelihood of avoidable cyber incidents and should be at the heart of service and infrastructure design and business culture.



Develop an incident response planning and exercising programme

Despite the obvious value of planning, documenting and testing incident response plans, few UK businesses have formal incident response plans in place, and even less have external communications plans.[5] Both of which are critical. Given that around a third of firms with response plans reportedly do not test them regularly[6], this is something that must be addressed to build greater resilience.

Understand your dependencies

It's vital that operators of critical infrastructure understand their dependencies. Learning from the incident in the summer of 2024, it's clear that organisations need to understand how they could be impacted by all of their suppliers and what risks that could present. Organisations also need to review their systems and operations to identify scenarios in which one single event could cause immediate widespread disruption. For their part, software vendors must go through the same process of learning, reviewing and adapting their update strategies to prevent future disruptions. By implementing rigorous testing and validation procedures prior to release, vendors can identify and address potential issues early. Adopting a phased rollout approach would also allow for real-world feedback and mitigate widespread impact.

Be prepared for the worst

Hoping for the best is not a strategy. Understanding the threat and factoring realistic worst case scenarios into financial and security planning is essential. Know what you'll do when something knocks out a critical dependency or key supplier, what you'll recover first to restore core services safely, and what can follow later.

Reference

1 Data Threat Report Critical Infrastructure Edition **(Thales, 2024)**

2 FBI says hackers preparing attack on US infrastructure **(Reuters, 2024)**; Cyber Security Advisory AA24-038A **(CISA, 2024)**

3 Data Threat Report Critical Infrastructure Edition **(Thales, 2024)**

4 Most common causes of sensitive information loss in worldwide organizations in 2023 **(Statista, 2024)**

5 **UK Cyber Security Breaches Survey 2024**

6 Special Editorial: with cybersecurity risks on the rise, some sectors can do more to prepare **(S&P Global 2023)**

We are Digital Intelligence

Digital Intelligence is home to over 4,700 digital, cyber and intelligence experts across 16 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared.

Our teams provide advanced digital capability, products and solutions that weave together digital threads of data so that customers get the vital insight they need – from the fine detail to the bigger picture, providing the power of perspective to confidently make the critical decisions that keep our societies safe and able to thrive.

Digital Intelligence is part of BAE Systems and has a rich heritage in helping to defend nations and businesses around the world from advanced threats. Whether on land, in the air, at sea, in space or cyberspace, we're your digital mission partner, with you every step of the journey.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS