Bridewell

Transforming cyber resilience through threat intelligence

Critical cyber security for critical organisations

Cyber Security	Managed Security	Penetration Testing	Data Privacy

bridewell.com

The systems that underpin our critical national infrastructure are under ever-increasing threat. Escalating geopolitical tensions, including recent Russian aggression against Ukraine, have given a renewed sense of urgency to the need to strengthen cyber defences against nation-state attacks.

Sectors particularly at risk include energy, chemicals, water, and transport. As well as their essential economic importance, these industries are constantly growing in interconnectivity, making them attractive targets for cyber criminals and state-affiliated hacking teams.

At the same time, new hybrid working patterns, coupled with the growing integration between IT and operational technology systems, are expanding attack surfaces. Operators must be hypervigilant to an ever-widening range of cyber risks and move to a position of assumed breach to increase maturity, focusing attention on improving detection and response through shared intelligence.

The growing threat of cyber warfare

Bridewell recently conducted research among 520 UK cyber security decision-makers in critical national infrastructure to understand cyber maturity levels, concerns and challenges within the industry.

Early findings include:

78%
are worried about the immediate threat of cyber warfare right now

1/4
worry that their systems are vulnerable to attack

MORE THAN
7 in 10
have seen cyber attacks increase since the start of the conflict

Despite great progress having been made across the industry since the introduction of NIS regulations, it’s clear evolving threats and geopolitical tensions are causing concern. Critical national infrastructure is - and always will - remain a key focus for political and financial attacks, so further steps must be taken to boost resilience and build cyber confidence.

Collaborating for the greater good

As attacks rise in sophistication and volume, operators of critical national infrastructure must collaborate more effectively in order to develop the threat intelligence needed to protect infrastructure and society.

According to Bridewell research, currently:

ONLY
1 in 5
have implemented threat hunting and cyber intelligence

ONLY
half
receive information about attacks through the disclosure of intelligence

LESS THAN
half
share their threat intelligence with peers

By consuming and sharing threat intelligence, organisations can better understand the threats they are likely to face – past present and immediate future - and move from a “reactive” to a proactive” security stance by expediting threat detection.

Use of threat intelligence is also critical in achieving compliance with the NIS regulations and the NCSC’s Cyber Assessment Framework.

Objectives A to D of the NIS regulations mandate that organisations have measures in place to:

- Manage risk in the organisation and supply chain
- Identify and manage vulnerabilities
- Implement monitoring to detect potential security problems and track the effectiveness of existing security measures
- Detect anomalous events in relevant network and information systems
- Ensure continuity of essential services in the event of system or service failure

All of which require cyber threat intelligence to improve maturity and build resilience.

NIS Regulations with Cyber Threat Intelligence

The NCSC developed the Cyber Assessment Framework to support operators of critical infrastructure in meeting the NIS Regulations. In includes the following which require threat intelligence to mature cyber resilience.

Managing Risk

- A1.a Board Directors
- A1.b Decision Making
- A2.a Risk Management Process
- A4.a Supply Chain

Protecting Against Cyber-Attacks

- B1.a Policy and Process Development
- B4.d Vulnerability Management

Detecting Cyber Security Events

- C1.a Monitoring Coverage
- C1.c Generating Alerts
- C1.d Identifying Security Incidents
- C1.e Monitoring Tools and Skills
- C2.a System Abnormalities for Attack Detection
- C2.b Proactive Attack Discovery

Minimising the Impact of Cyber Security Incidents

- D1.a Response Plan
- D1.c Texting and Exercising
- D2.a Incident Root Cause Analysis
- D2.b Using Incidents to Drive Improvements

Using threat intelligence

Cyber threat intelligence is key to building a proactive threat-led cyber defence capability and can significantly improve your state of readiness to prevent, detect and respond to attacks.

1. Understand what's important to your organization - if you don't you won't know who's potentially targeting you, their motivations, or the TTPs they may deploy.
2. If you don't have a cyber threat intelligence capability, look to engage with a third party to help identify the cyber assets most critical to business continuity.
3. Start simple with intelligence and identify intelligence collection sources (both structured and unstructured) that allow you to build your own intelligence database.
4. Use the MITRE ATT&CK framework to work out the potential tactics and techniques attackers may use. Align these to your defensive capabilities, identifying any gaps (exposure) and how to address them.
5. As your intelligence matures, use it to inform decisions at all levels of the organisation.

Anticipating future risks

In the future, as the scale of threats grows, it is likely we will see nation-states collaborating across borders within a cyber agreement aligned to the physical space. And while complete prevention of cyber attacks is not possible, critical national infrastructure can be designed to be more cyber resilient.

Operators of critical infrastructure need clear, contextual intelligence about active cyber attacks by which they may be targeted and the forms they might take to strengthen resilience. Investing in threat-led security operations can empower organisations to develop a 360-degree picture of their threat landscape and enable vulnerability and risk management strategies to be structured more effectively.

Armed with the right intelligence, security teams can conduct richer security investigations and mount an effective response, regardless of what threats come their way.

To find out more about Bridewell's Cyber Threat Intelligence service visit:
www.bridewellconsulting.com/cyber-threat-intelligence

To register to receive Bridewell's full research report get in touch at research@bridewell.com

About Bridewell

Bridewell is a cyber security services company that specialises in protecting the data and reputation of organisations in highly regulated industries, such as critical national infrastructure and financial services.

The company's services span cyber security, penetration testing, data privacy and fully managed security services, with its 24/7 Security Operations Centre trusted to protect some of the UK's most critical national infrastructure.

Its team of diverse, highly-skilled consultants have a deep-rooted understanding of both Operational Technology (OT) and Information Technology (IT) environments, helping critical organisations to drive strategic change securely, reduce risk and build cyber resilience amid rising cyber threats.

Assured Service Provider
in association with
National Cyber
Security Centre

CREST
VA
PEN TEST
SOC

UK Civil Aviation Authority
ASSURE

SNR CERTIFICATION ISO/IEC 27001
UKAS MANAGEMENT SYSTEMS 8327
Trading name of SN Registrars (Holdings) Ltd

SNR CERTIFICATION ISO 9001
UKAS MANAGEMENT SYSTEMS 8327
Trading name of SN Registrars (Holdings) Ltd

The Certification Group Limited
TCG
27701:2019

PCI Security Standards Council

Crown
Commercial
Service
Supplier

IASME CONSORTIUM
CYBER ESSENTIALS

Member of
Microsoft Intelligent
Security Association
Microsoft

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

Ecologi
climate
positive
workforce

☎ +44 (0)3303 110 940

✉ hello@bridewell.com

bridewell.com

Bridewell