Water Utilities - Challenges in Managing your Cyber Risk.

qldwater 2024 Annual Forum

Andrew Morgan, Australia/New Zealand Cyber Security Consulting Leader

23 August 2024

wtw

1

Today's Session

1. **Cyber Security** – Threats and trends.
2. **Boards and Execs** – What do they need to know.
3. **Cyber Security Risk Management** – Doing what matters most
4. **Cyber Insurance** – What does this mean for you?

wtw

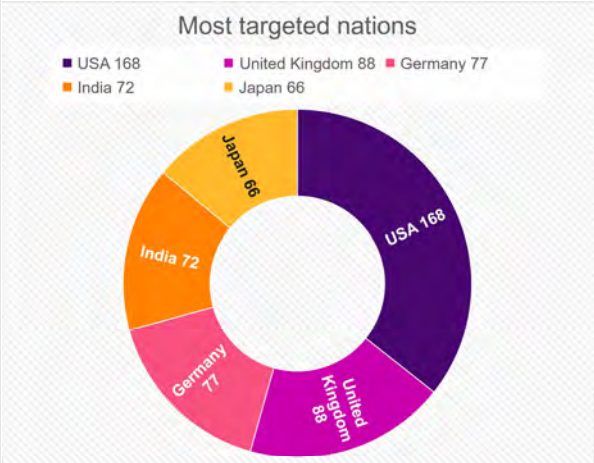
2

Cyber Security – Threats and trends.

wtw

3

Cyber Security – 2024 Threats and trends.



wtw

4

Cyber Security – 2024 Threats and trends.

wtw 5

5

Cyber Security – 2024 Threats in the Water Industry.

IT and OT were two different worlds....

IT

- Business
- Operations
- Enterprise systems

Systems to store, retrieve, transmit, and manipulate data or information

OT

- Machines
- Processes
- Systems within a plant

Detect/cause a change in the operational environment based on dedicated hardware and software

Now converging into a truly digital environment

- Web – based deployments
- ERP
- Software and hardware
- Cloud infrastructure

Business insights

IT — Creating connected & secure environment — OT

- SCADA
- RTU/PLC
- HMI
- Physical equipment
- Embedded technologies
- Machinery

Operational insights

Connected IT & OT departments

Uniform converged IT-OT platform – process, tools & governance

Improved automation and visibility into distributed OT

wtw 6

6

Boards and Execs – What do they need to know.

Boards and Execs – What do they need to know.

Are we OK?

Basic questions that CISOs need to answer for the board and C-suite:

1. What are the risks we are facing?
2. What is the cybersecurity team doing about it?
3. Does the team have what it needs to make the right decisions and act quickly?
4. Are company assets, data, and systems secure?
5. How would we know if we have been breached?
6. How does our security program compare to other companies in the industry?
7. Do we have enough resources for our security program?
8. How effective is our program; is our investment correctly aligned?

Cyber Security Risk Management – Doing what matters most

Cyber Security Risk Management
Doing what matters most

Nobody can protect every asset

Protect the Crown Jewels!!

What are the crown jewels?

How do you define them?

What are the dependencies for each of the crown jewels?

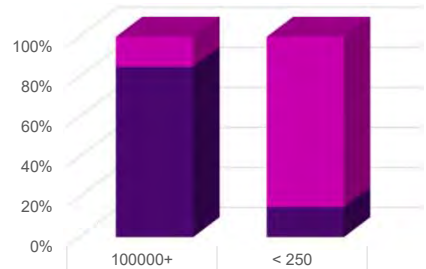
Do you have a critical assets register?

What are the threats that could impact the crown jewels?

Cyber Insurance – What does this mean for you?

Cyber Insurance
What does it mean for you?

Organizations that carry cyber insurance by number of employees



	100000+ employeees	< 250 employees
Do not have cyber insurance	15%	85%
Have cyber insurance	85%	15%

Organisations having cyber insurance by revenue.
High Revenue > $5.5 billion USD year
Low Revenue < $250 million USD year

	High revenue organisations	Low revenue organisations
Do not have cyber insurance	25.45%	75.38%
Have cyber insurance	74.55%	24.62%

WEF Global Cybersecurity Outlook 2024

Cyber Insurance market update – H2 2024

Pricing guidance

Pricing trends improved in 2023 and market stability has continued in 2024.

- **Q1 2023** +0% to +20%
- **Q2 2023** -0% to +10%
- **Q3 2023** -5% to +5%
- **Q4 2023** -5% to flat
- **Q1 2024** -5% to flat
- **Q2 2024** -5% to flat
- **Q3 2024** flat (prediction)

(clients maintaining mature cyber security posture and clean loss history have better results)

Capacity and coverage

Plenty of capacity in the market with some primary markets willing to deploy $10m+ (depending on class of business and security posture).

Although the threat of cyber warfare continues to be a topic, more markets are showing flexibility when it comes to war exclusions.

We continue to monitor how clients are using artificial intelligence and how markets are addressing coverage for the new exposures AI has created.

Underwriting process

Ransomware supplementals are still being required by primary carriers.

Third party security ratings are now commonly part of the underwriting process (BitSight, Security Scorecard, Cyence).

Underwriting calls preferred for large risks.

Carrier risk engineers commonly are joining underwriting calls.

Additional underwriting questions on biometric data collection, AI usage and meta-pixel tracking technology exposure.

Cyber Insurance
Focus areas for underwriters

Remote desktop protocol

RDP is a dominant attack vector for ransomware. Recommendations to improve RDP security include:

- VPN
- Encryption
- MFA
- RDP gateway
- Network level authentication
- Complex passwords
- Enable restricted admin mode
- Restrict access via a firewall

Multi-factor authentication

In addition to RDP, insurers look for insureds to utilize MFA to improve security for:

- Email
- Remote network access
- Privileged user accounts
- Other virtual desktop instances (VDI)
- Cloud resources including Office365

Additional safeguards/concerns

- Third-party vendor management program
- Network Level Authentication (NLA)
- Endpoint Detection Protection and Response
- Limit Domain Administrator/Service Account Access
- Minimize number of Local Admin Accounts and ensure each is unique
- Regular cybersecurity awareness and phishing training
- If using O365, O365 Advanced Threat Protection add-on and Defender
- Use account-naming convention that does not reveal organizational info.
- 24/7 SOC or MSSP solution
- PAM Solution
- Email Security Pre-Scan, SPF, DKIM, DMARC
- Asset management
- Access management
- Systemic Vulnerability Management (e.g. Solarwinds, Log4J)
- Legacy systems/End of Support – proper compensating controls
- Network Segmentation
- Patching cadence / policy
- SIEM – event monitoring and log management
- AI utilization
- Meta pixel/tracking technologies exposure

Backup and response

Properly secured backups reduce the severity of Ransomware losses. Recommendations include:

- Encrypting backups
- Segregating backups; physically stored offsite and offline
- Regular testing backups for data integrity and restorability
- Regularly performing full and incremental backups of data
- Regular testing of incident response/business continuity plans including ransomware and tabletop exercises