Partners in Performance®
Unleashing potential | Lasting impact

PiP Speak

# Cybersecurity: Are you protecting your critical assets?

## Executive summary

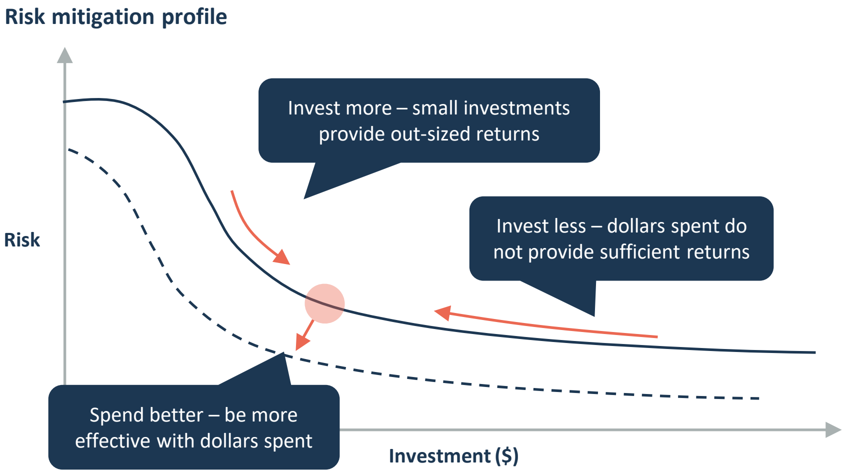
Since the coronavirus pandemic began, cyber attacks have increased dramatically around the globe. A top United Nations official reported a 600% increase in malicious emails during this period, with a cyber attack taking place an average of every 39 seconds. The damage from ransomware attacks alone is expected to reach $20bn in 2021 – almost double the cost in 2019 – and businesses are expected to fall victim to a ransomware attack every 11 seconds by that time, up from every 40 seconds in 2016.

These threats have been more common internationally, increasing in many countries and unfortunately are here to stay. Companies that have been brought to their knees will invariably mention that they scored well on cyber audits. How is this possible?

Too often, cyber strategies focus on complying with best practices rather than on protecting 'value', with significant attention dedicated to Information Technology (IT). Meanwhile, Operations Technology (OT), the technology that runs your operations, is neglected. This is a clear signal that the cybersecurity plan did not start with a clear understanding of value, risk or cyber strategy.

A sound cybersecurity strategy should start by understanding how critical each of your physical and data assets are, what cyber threats could compromise these assets and how likely this is to occur. This enables teams to develop mitigation plans and determine the associated value and costs. Without this value focus, many strategies are like spreading peanut butter on toast – evenly spread, rather than focussing on the at-risk assets.

Cyber investment decisions should make informed trade-offs between value and risk



When looking at your organisation's cybersecurity strategy, it is crucial to rigorously review three questions:

1. What are the most valuable, vulnerable and threatened things that must be protected?
2. What is needed to protect our at-risk assets?
3. How do we know we are protecting our valuable assets effectively?

## 1. What are the most valuable, vulnerable and threatened assets to protect?

Your organisation needs to understand how it delivers value, and what needs to be protected to realise that value and avoid incurring the expense of recovering from a cyber attack.

We offer pointers around the elements that should be covered by your cyber strategy:

### Mapping your organisation's assets (both physical and data) enables you to understand:

- Data entry and exit points for each asset, including interconnectivity between assets and between platforms
- Significance to your business if this asset was compromised or had connected systems and processes infected

### Individual systems and interconnectedness between systems is assessed to identify weaknesses

○ Highly vulnerable ● Limited vulnerability

| Value chain | Mine | Processing | Rail | Port |
|---|---|---|---|---|
| Input/control systems | ◐ | ◐ | ● | ○ |
| Output/data capture | ● | ○ | ● | ○ |
| Data aggregation and viewing | ● | ● | ● | ● |

For each important asset, you can develop a view on whether it is at-risk by assessing both threat and vulnerability.

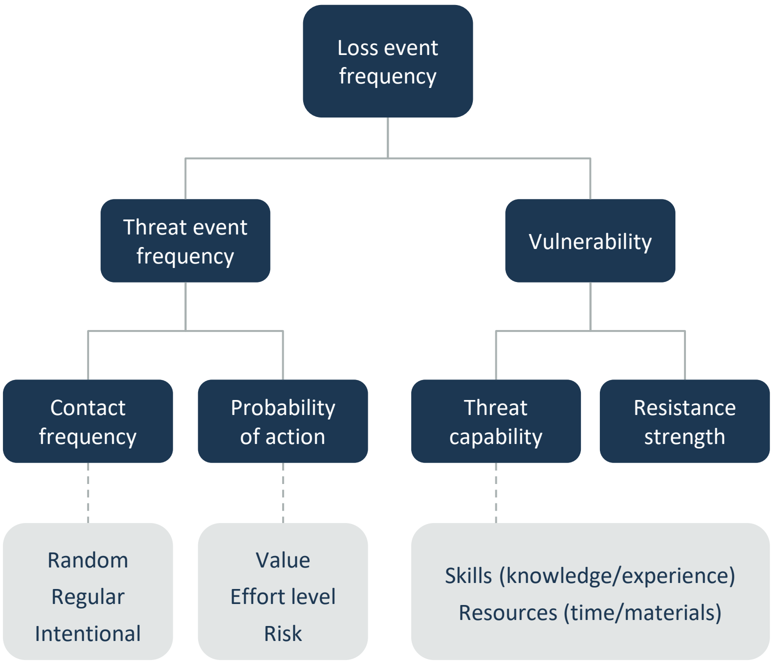
### **Threat:** What cyber actors have the desire and capability to attack us?

- Desire: What incentives do cyber actors have to compromise our critical elements? This is derived from threat intelligence and combined with an understanding of the organisation's context and industry.
- Capability: What are the 'bad guys' capable of? This is derived from threat intelligence and analysis of recent events.

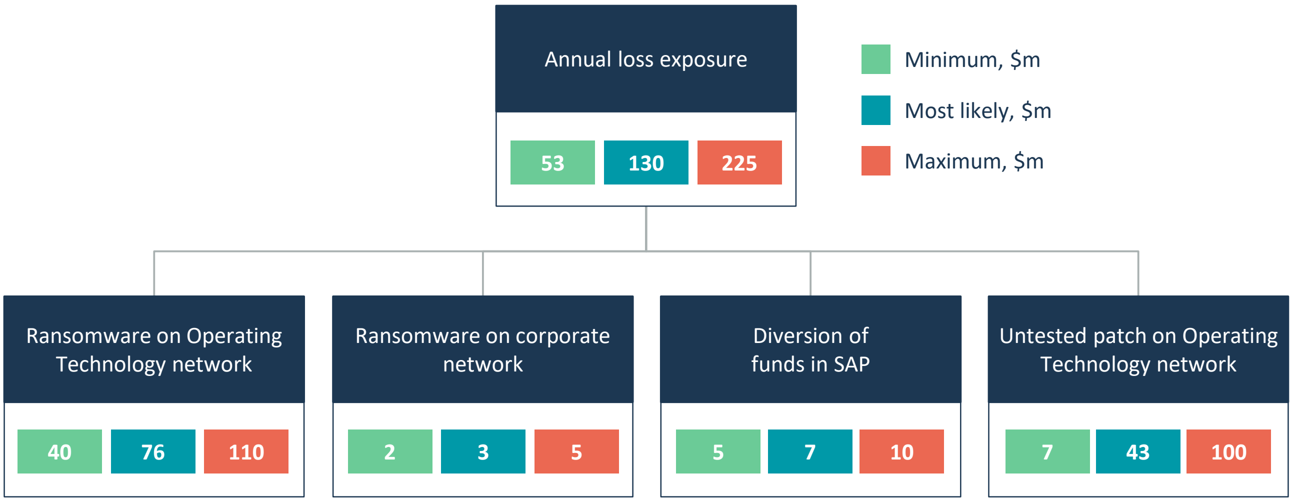
### **Vulnerability:** How likely is a threat?

With an understanding of threats, capability and your current cybersecurity levels, Operations, Finance, Risk and IT can work together and quantify your vulnerability and the financial risk of a successful cyber attack.

### Threat/vulnerability assessed for each asset



Sample cyber risk output of FAIR[1] model analysis

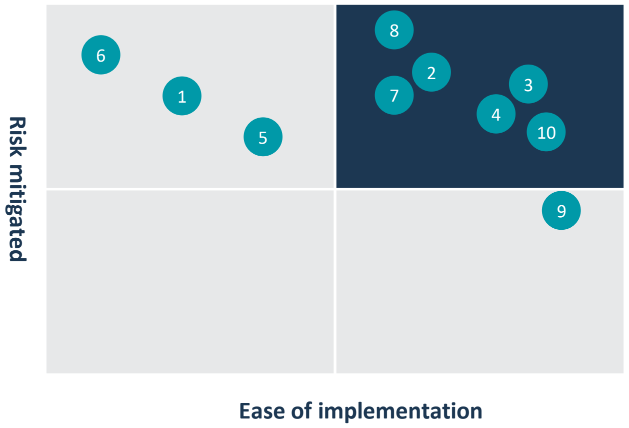

Annual loss exposure
53
130
225
🟩 Minimum, $m
🟦 Most likely, $m
🟥 Maximum, $m
Ransomware on Operating Technology network
40
76
110
Ransomware on corporate network
2
3
5
Diversion of funds in SAP
5
7
10
Untested patch on Operating Technology network
7
43
100

## 2. What is needed to protect our valuable, at-risk assets?

These analyses guide your technical teams in determining the required processes, systems and disciplines that need to be established within the organisation. This will include both technical and behavioural solutions, which trade-off potential mitigation value against both cost and ease of implementation.

These solutions can then be prioritised by the likely impact each idea or group of ideas will have on the magnitude of loss associated with that asset. Combined with the mitigation cost, this leads to further prioritisation based on the expected impact of mitigation strategies.

Sample ideas from cyber assessment triage



1. Invest in patches for third-party system vulnerabilities
2. Two-factor authentication to critical assets
3. Implement cybersecurity training programme at all levels
4. Provide cybersecurity training for IT personnel who demonstrate aptitude in cyber
5. Procure and implement cybersecurity tools for monitoring network traffic
6. Architect virtual contingency operations options for the ROC
7. Join the Mining and Metals Information Sharing Analysis Center (MM-ISAC)
8. Next-generation network segmentation
9. Intelligence-based threat briefings
10. Conduct regular spear phishing tests

With a clear understanding of your vulnerabilities, risks and priority actions, your organisation can define a roadmap to cybersecurity. This will include a series of agreed initiatives and programs to improve your technical protection and resilience, while also training and coaching your entire organisation on how to stay cyber safe.

[1] The FAIR model, developed by the FAIR Institute (https://www.fairinstitute.org/), uses Factor Analysis of Information Risk to determine the value at risk from a cyber incident.

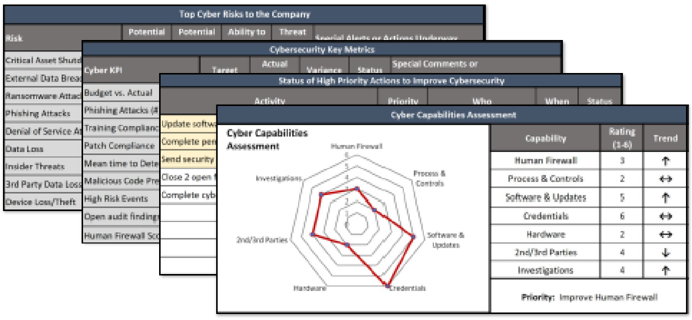
### 3. How do we know we are protecting our at-risk assets effectively?

While cyber audits are useful to remain compliant with regulations and best practices, compliance alone does not deliver security, particularly when situations are rapidly evolving.

Your cyber strategy and execution should prioritise and protect the critical systems and data assets that power your operation. This will include tracking of actions required to position your organisation to defend critical assets, an overview of threats manifesting and any trends on how well the established defences are coping.

Unfortunately, common cyber KPIs often focus on ‘how dangerous it is out there’ (e.g. number of phishing emails received, number of external scans against the network), rather than whether the organisation is exposed or effectively protecting its at-risk assets. By shifting the focus of your KPIs (e.g. from ‘number of external scans against the network’ to ‘number of failed logins’), your organisation will gain a better understanding of potential target attacks, enabling it to act to protect itself. If you know that failed logins are increasing, you can identify which usernames and passwords may have been leaked outside the organisation, then focus efforts to increase security of those accounts and improve the training of those individuals affected.

Actionable C-Suite dashboard highlights variances



Top Cyber Risks to the Company

| Risk | Potential | Potential | Ability to | Threat | Special Alerts or Actions Underway |
|---|---|---|---|---|---|
| Critical Asset Shutd | | | | | |
| External Data Brea | | | | | |
| Ransomware Attac | | | | | |
| Phishing Attacks | | | | | |
| Denial of Service A | | | | | |
| Data Loss | | | | | |
| Insider Threats | | | | | |
| 3rd Party Data Loss | | | | | |
| Device Loss/Theft | | | | | |

Cybersecurity Key Metrics

| Cyber KPI | Target | Actual | Variance | Status | Special Comments or |
|---|---|---|---|---|---|
| Budget vs. Actual | | | | | |
| Phishing Attacks (# | | | | | |
| Training Complianc | | | | | |
| Patch Compliance | | | | | |
| Mean time to Dete | | | | | |
| Malicious Code Pre | | | | | |
| High Risk Events | | | | | |
| Open audit finding | | | | | |
| Human Firewall Sc | | | | | |

Status of High Priority Actions to Improve Cybersecurity

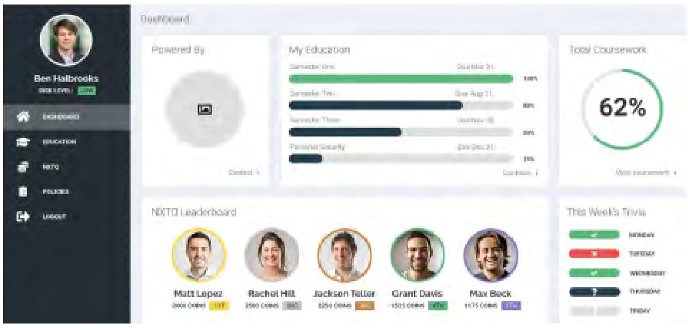
| Activity | Priority | Who | When | Status |
|---|---|---|---|---|
| Update softw | | | | |
| Complete pen | | | | |
| Send security | | | | |
| Close 2 open | | | | |
| Complete cyb | | | | |

Cyber Capabilities Assessment

| Capability | Rating (1-6) | Trend |
|---|---|---|
| Human Firewall | 3 | ↑ |
| Process & Controls | 2 | ↔ |
| Software & Updates | 5 | ↑ |
| Credentials | 6 | ↔ |
| Hardware | 2 | ↔ |
| 2nd/3rd Parties | 4 | ↓ |
| Investigations | 4 | ↑ |

**Priority:** Improve Human Firewall

Clickable deep-dive dashboards build accountability



## Conclusion

Nothing can eliminate your cyber risk. However, a thoughtful, risk-informed and business-driven cyber strategy will enable your organisation to stay focussed on the priorities, make better decisions and focus funds on the most important areas to protect. You don’t need to be a cybersecurity expert to be an effective partner in the process, as your organisation moves beyond compliance and towards real security and value protection.

Key questions to ask:

- → Where is your organisation most vulnerable?
- → What are your main risks, and what is the cost if those risks eventuated?
- → How much can these risks be mitigated and at what price?
- → Are your cyber activities prioritised on the expected impact and cost?
- → Do KPIs and dashboards reflect the agreed cyber strategy?
- → Is your current cyber strategy effective?

### About the authors

Jason Israel leads our Australian cyber practice and is a former Pentagon cyber advisor and member of the Obama White House National Security Council.

Major General Patricia Frost, U.S. Army Retired, was the first Director of Cyber, Electronic Warfare, and Information Operations for the Department of the Army and has extensive cyber experience.

Partners in Performance helps clients unleash their true potential – at a business, commercial and people level. Working as close partners, we enable our clients to achieve game-changing results that drive lasting impact. Contact us to find out more: pip.global info@pip.global