SecureTeam

CYBER RISK: A FUELLING INDUSTRY PERSPECTIVE

JOINT INSPECTION GROUP

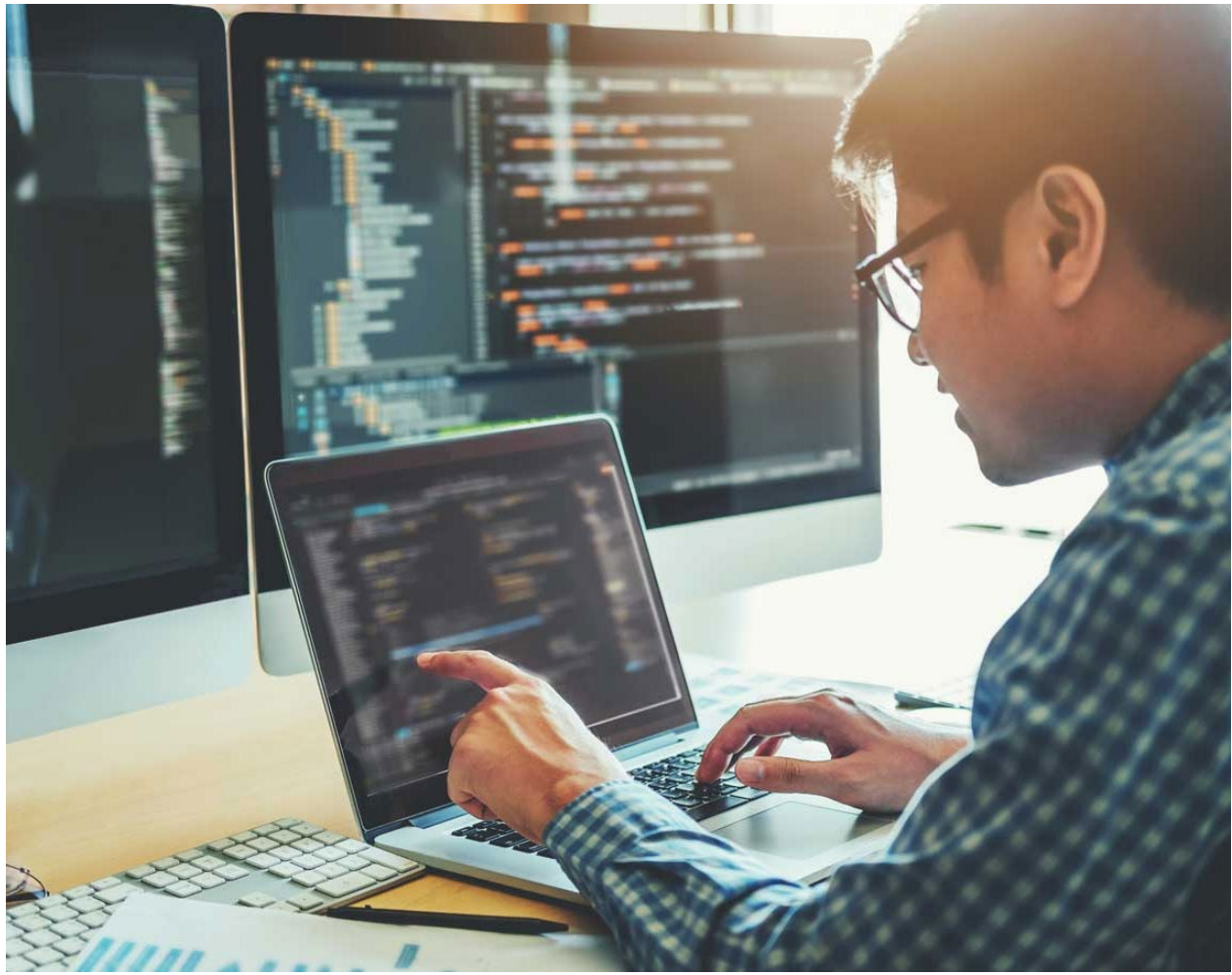
information. secured.

IAN REYNOLDS – DIRECTOR & PRINCIPAL CONSULTANT

- Started life as an Electronic & Electrical Engineer
- 15 Years in SCADA development & integration
- Built embedded control systems & ROVs
- Moved into Penetration Testing in 2010
- Founded SecureTeam in 2016

AVIATION CYBER SECURITY EXPERTS

- UK-based Cyber Security Practice
- 25+ Years Industry Experience
- Penetration Testing Specialists
- Governance, Risk & Compliance Consultancy
- SCADA & Hardware Security Experts
- CREST Accredited
- ISO 9001 & 27001 Certified
- Security Cleared Consultancy Team



OUR CLIENTS


UK
Parliament


NHS


RICOH
imagine. change.


EXCLUSIVE
NETWORKS


animal
friends
Pet Insurance


united
international
pictures


MENZIES
AVIATION


Preventx
Integrated Diagnostics


NUTANIX


WP engine


Royal College
of Surgeons
of England


ACTEMIUM


FRESENIUS
MEDICAL CARE


IATA


Tamr


gasrec

Cyberattacks on aviation surged 600% in 2025 compared with 2024, according to IATA

AVIATION CYBER ATTACKS ARE SOARING TO AN ALL TIME HIGH

- Cyberattacks on aviation surged **600%** in 2025 compared with 2024 (Source: IATA)
- Ransomware attacks on the oil and gas industry rose **935%** between April 2024 and April 2025. Aviation fuelling is directly affected by this. (Source: Zscaler ThreatLabz Report 2025)
- A 2025 Trustwave report found **84%** of energy sector incidents start via phishing and **96%** involve remote service exploitation (Source: Trustwave SpiderLabs Report 2025)

Cyberattacks on aviation surged 600% in 2025 compared with 2024, according to IATA

CYBER ATTACK – COLLINS AEROSPACE (SEPT 2025)

- Ransomware attack of Collins Aerospace's MUSE check-in and boarding platform, forcing major hubs including London Heathrow, Brussels, Berlin, and Dublin to revert to manual processing, with more than 100 flights delayed or cancelled.
- The attack hit the shared software provider whose check-in and baggage software multiple airlines rely on.
- The Russia-linked Everest extortion group claimed responsibility and threatened to release around 1.5 million records, including passenger data, said to be stolen from Dublin Airport.

Cyberattacks on aviation surged 600% in 2025 compared with 2024, according to IATA

CYBER ATTACK – KUALA LUMPUR AIRPORT (MARCH 2025)

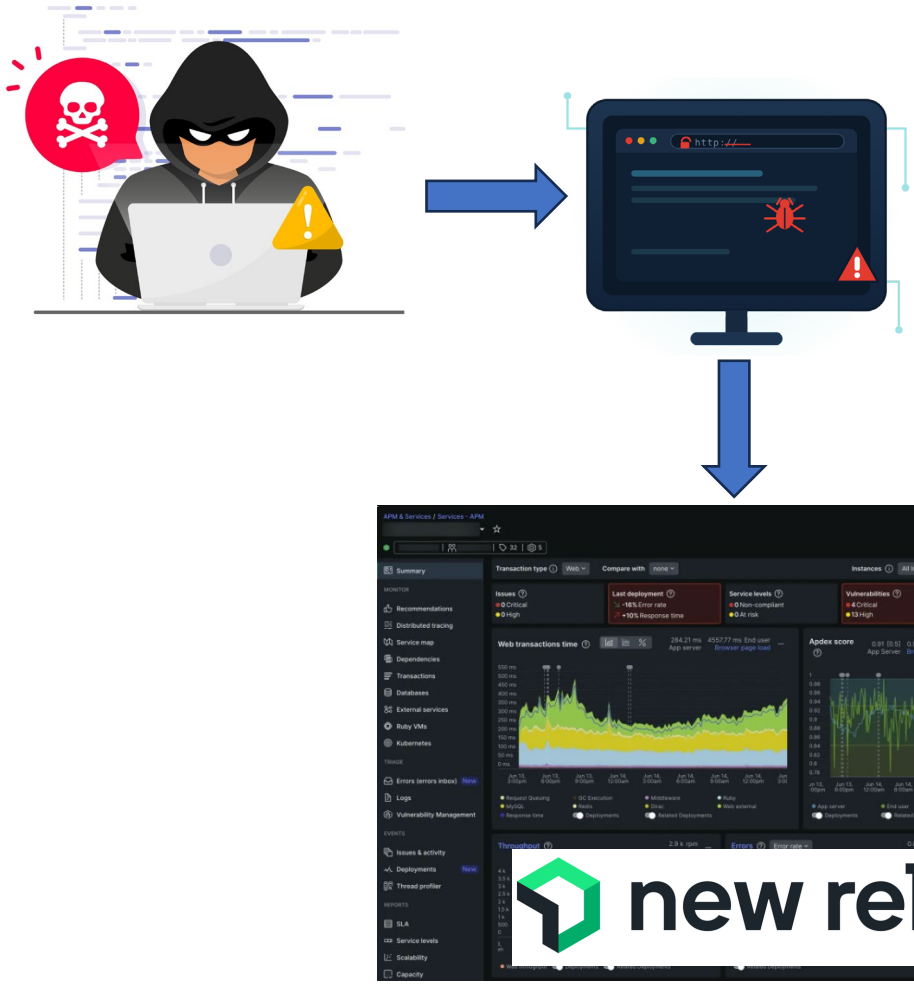
- Cyberattack disrupted KLIA's flight information displays, check-in counters, and baggage handling.
- Staff resorted to writing departure times on whiteboards (?!?!?)
- Attackers demanded $10 million, which Prime Minister Anwar Ibrahim rejected outright.
- The Qilin ransomware group claimed responsibility and said it stole 2 TB of data.
- Qilin has repeatedly targeted the aviation sector over the past 5+ years.

COMPROMISED AIRPORT BOOKING WEBSITE

- Airport Lounge Booking & Concierge Website
- Outdated Magento CMS - Last updated 2010
- SQL Injection vulnerability allowed database access

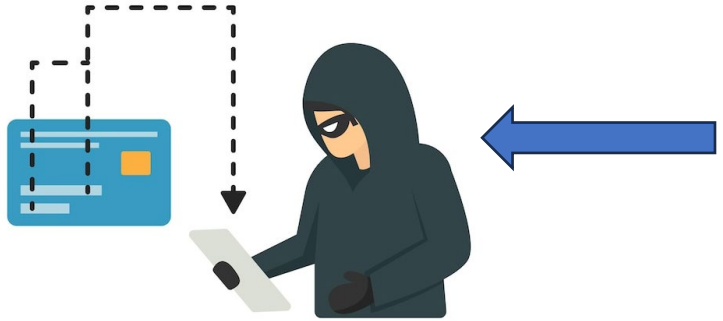
COMPROMISED AIRPORT BOOKING WEBSITE

- Airport Lounge Booking & Concierge Website
- Outdated Magento CMS - Last updated 2010
- SQL Injection vulnerability allowed database access
- Attacker inserted New Relic Web Monitoring Tool code into payment form to copy the cardholder information

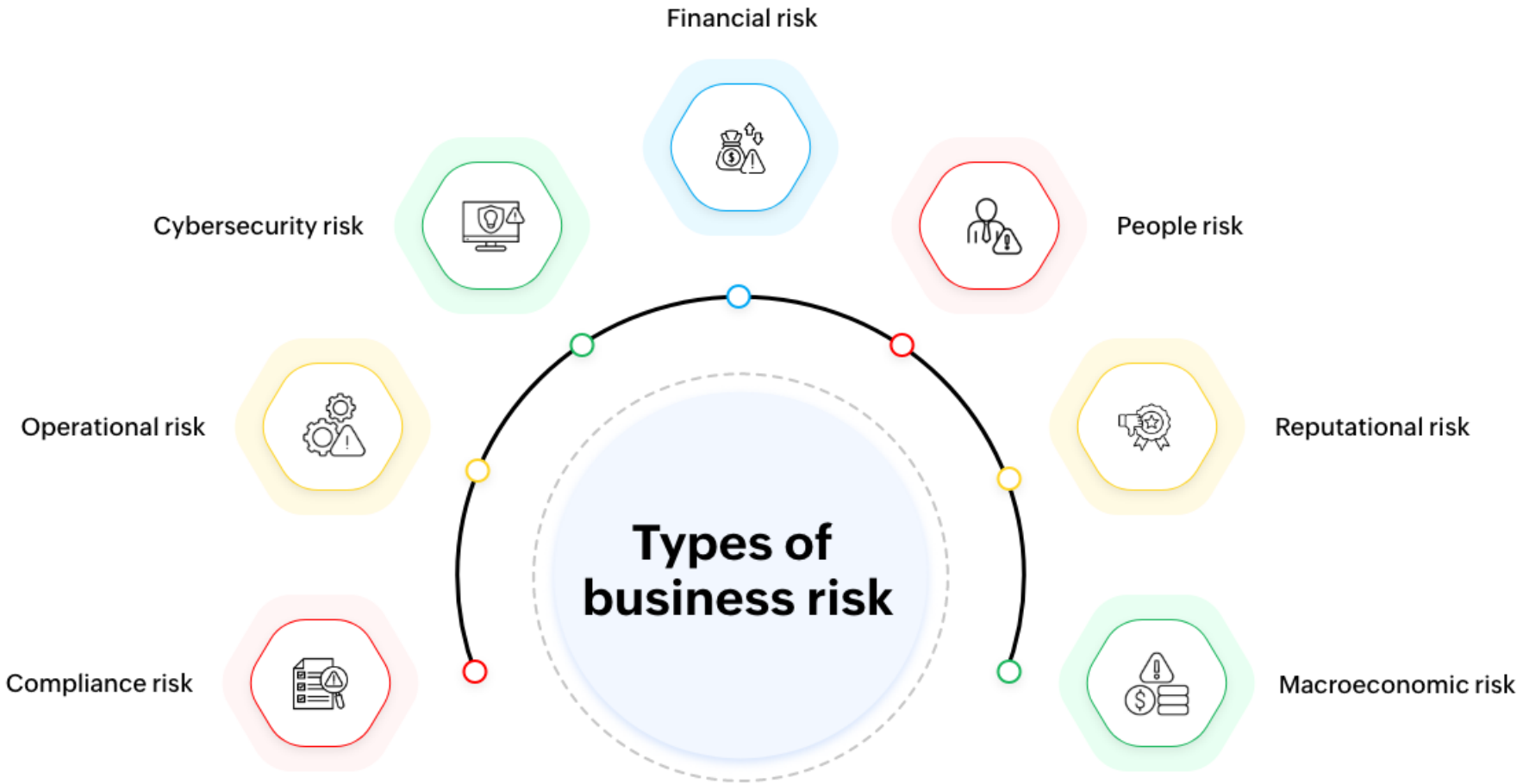


COMPROMISED AIRPORT BOOKING WEBSITE

- Airport Lounge Booking & Concierge Website
- Outdated Magento CMS - Last updated 2010
- SQL Injection vulnerability allowed database access
- Attacker inserted benign code into credit card payment form
- New Relic Web Monitoring Tool used to copy cardholder information
- ~£36m Annual Transactions

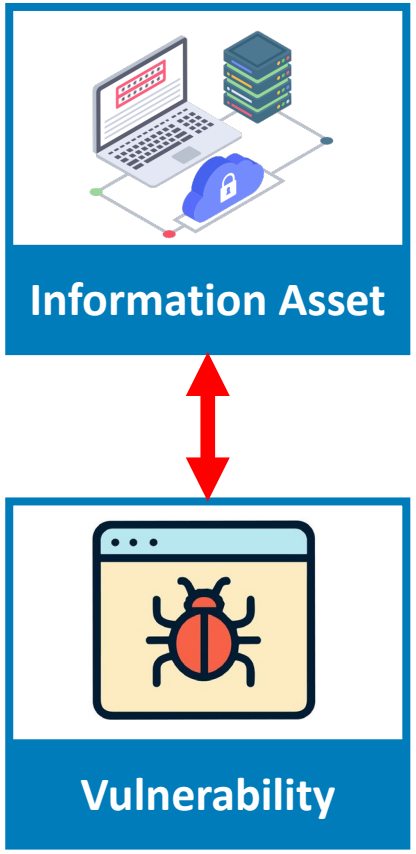


CYBER THREATS ARE A BUSINESS RISK

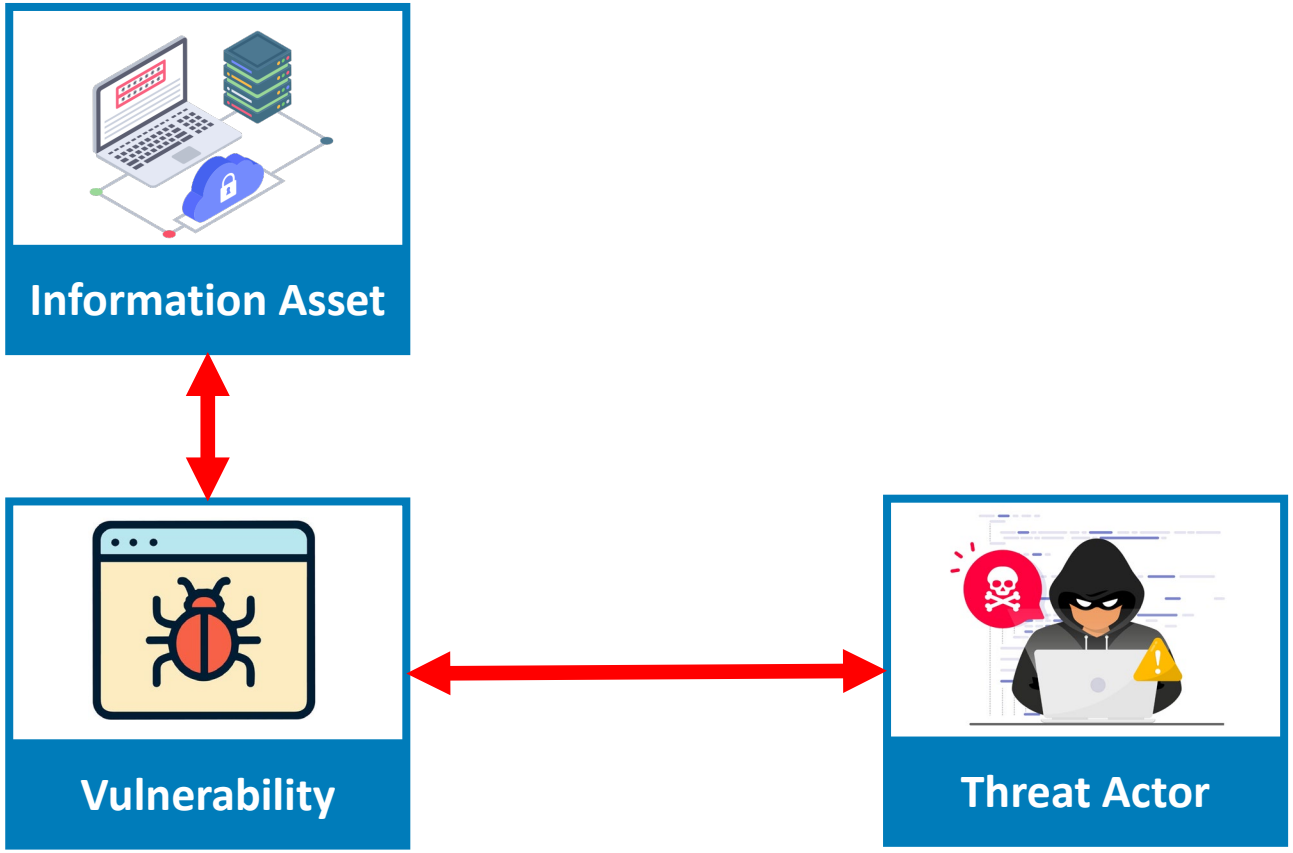


CALCULATING CYBER RISK – INFORMATION ASSET

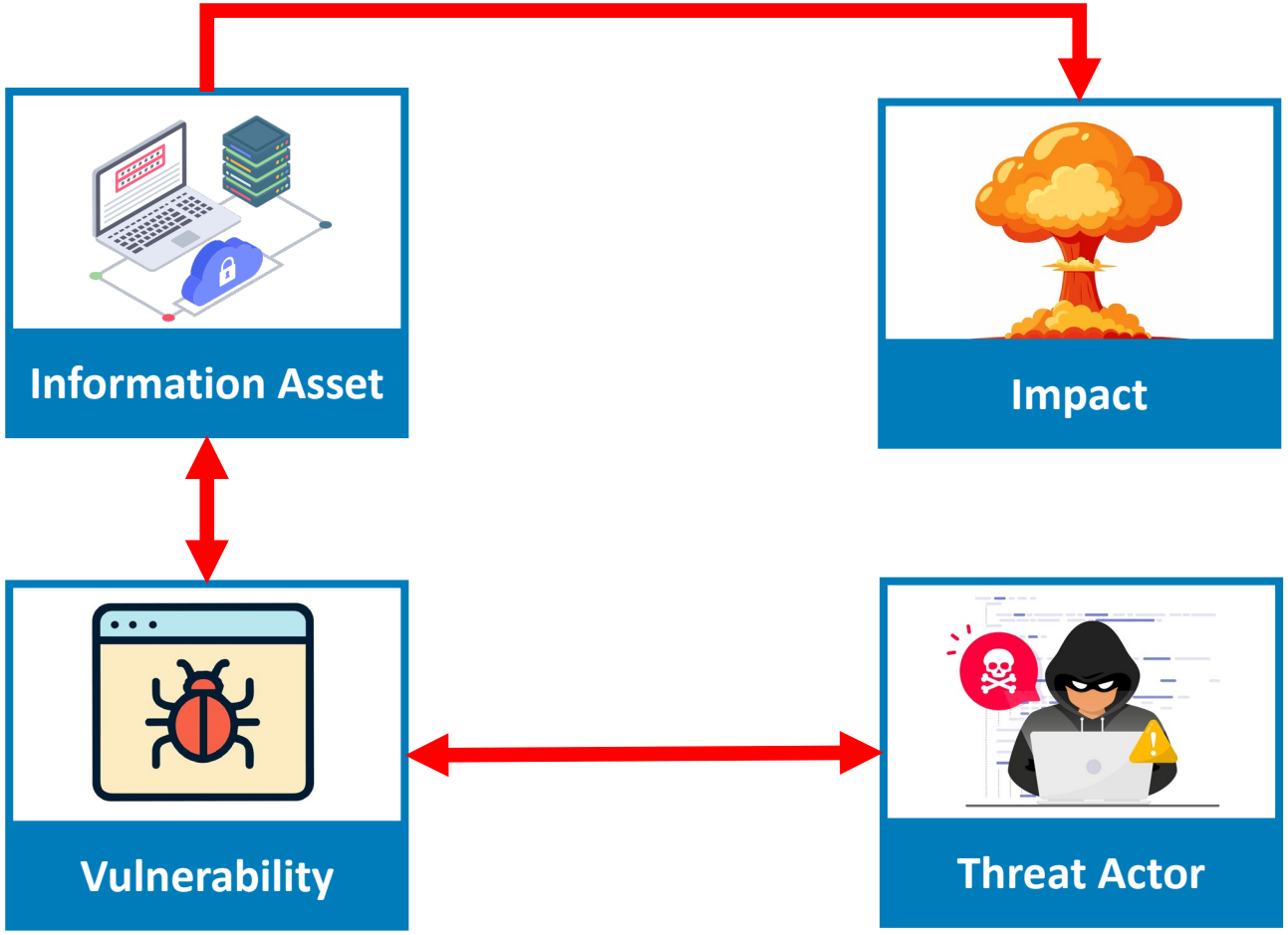
CALCULATING CYBER RISK - VULNERABILITY



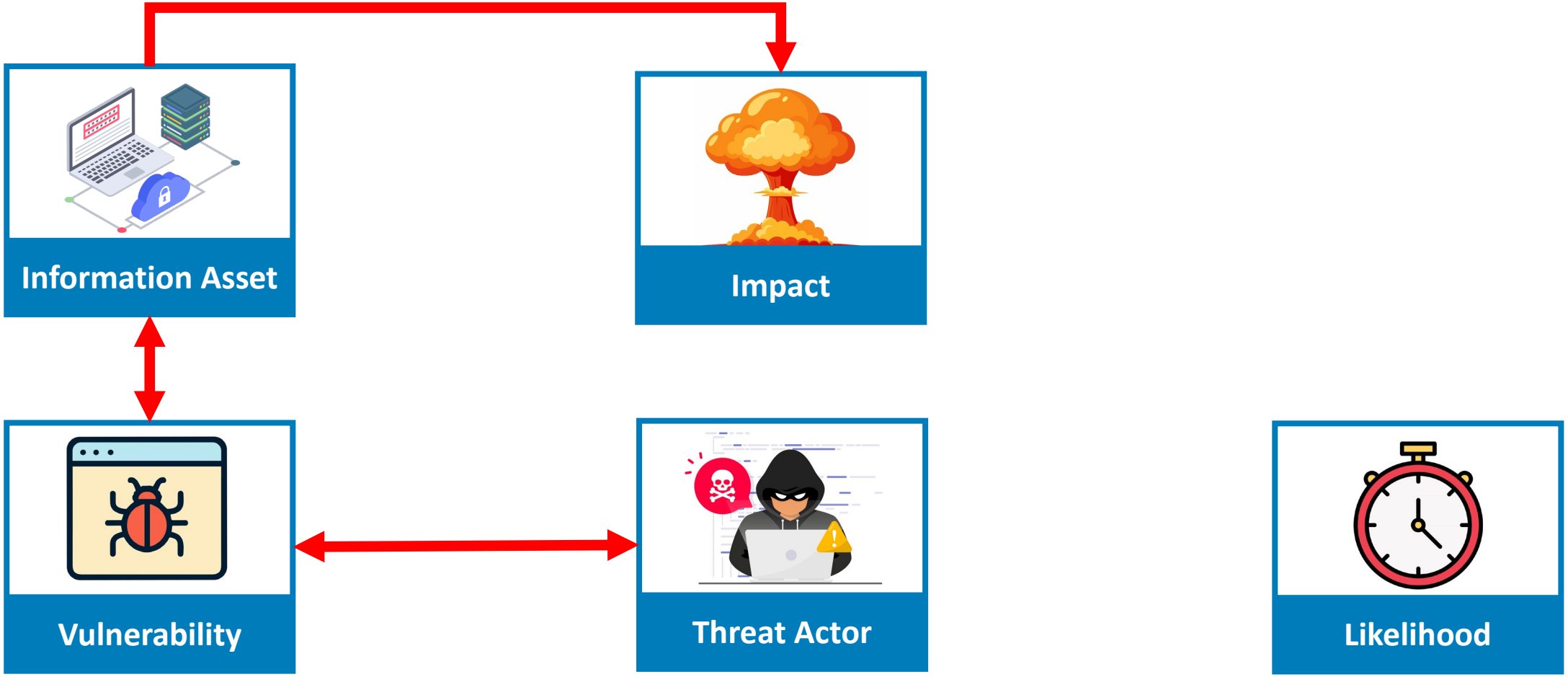
CALCULATING CYBER RISK – THREAT ACTOR



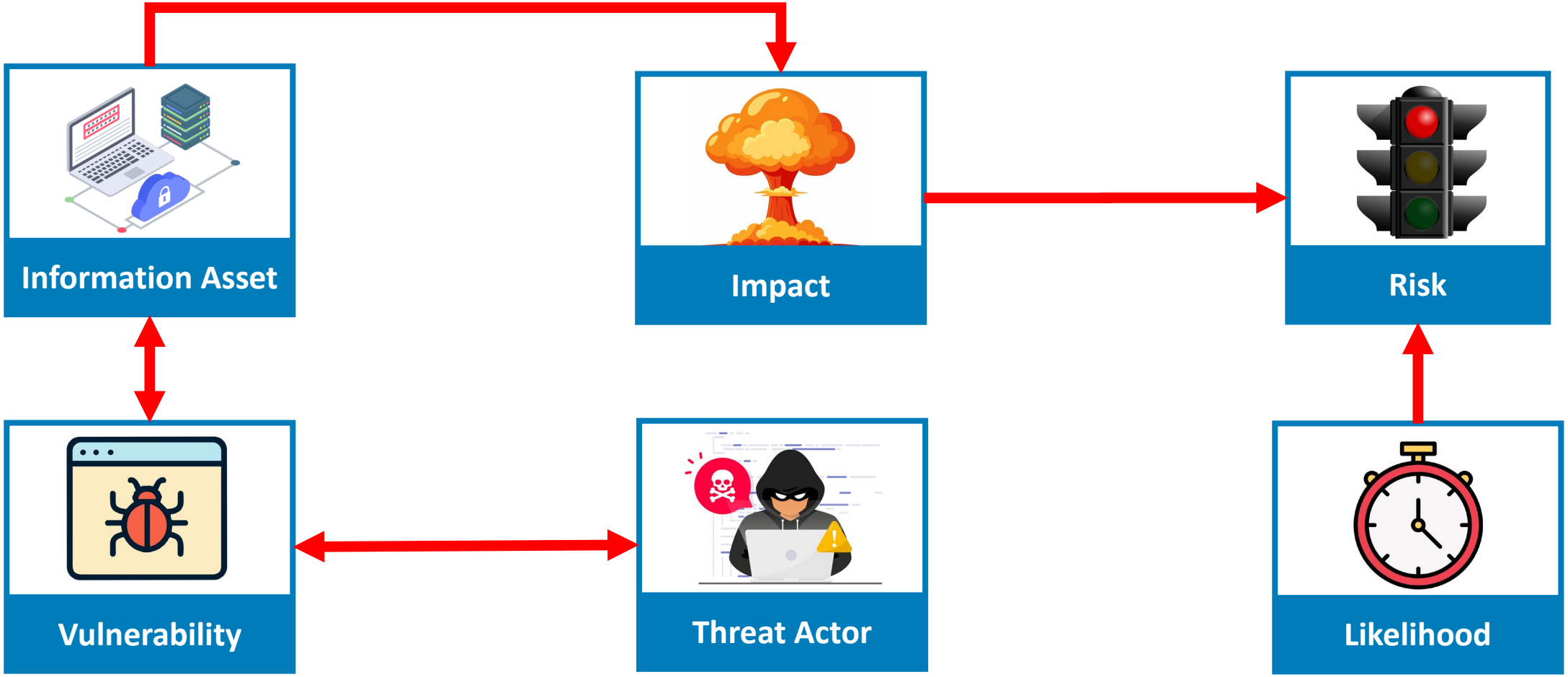
CALCULATING CYBER RISK - IMPACT



CALCULATING CYBER RISK - LIKELIHOOD



CALCULATING CYBER RISK – RISK SCORE



RISK = IMPACT x LIKELIHOOD

INFORMATION ASSETS

- Customer and client data
- Employee and HR records
- Financial information
- Intellectual property and trade secrets
- Legal and compliance records
- Servers and data storage
- Workstations and laptops
- Network equipment
- Mobile devices
- Removable media
- Infrastructure and facilities

AVIATION FUELLING INFORMATION ASSETS

Information

- Commercial pricing
- Contracts
- Into-plane records
- Payroll Information
- Training Records
- Fuel Batch Certificates
- Planned Maintenance Checklists
- Vehicle Service History
- Near-Miss Reports
- Operating Manuals
- Technical Diagrams
- Maintenance Logs

Information Technology

- Workstations
- Servers
- Databases
- Firewalls
- Printers
- Document Scanners
- BYOD Devices
- Tablets
- Network Switches
- Wireless Access Points
- Clock-In Machines
- Internet Service Provider
- Fuel Stock Control Server
- Door Access Control

SaaS Services

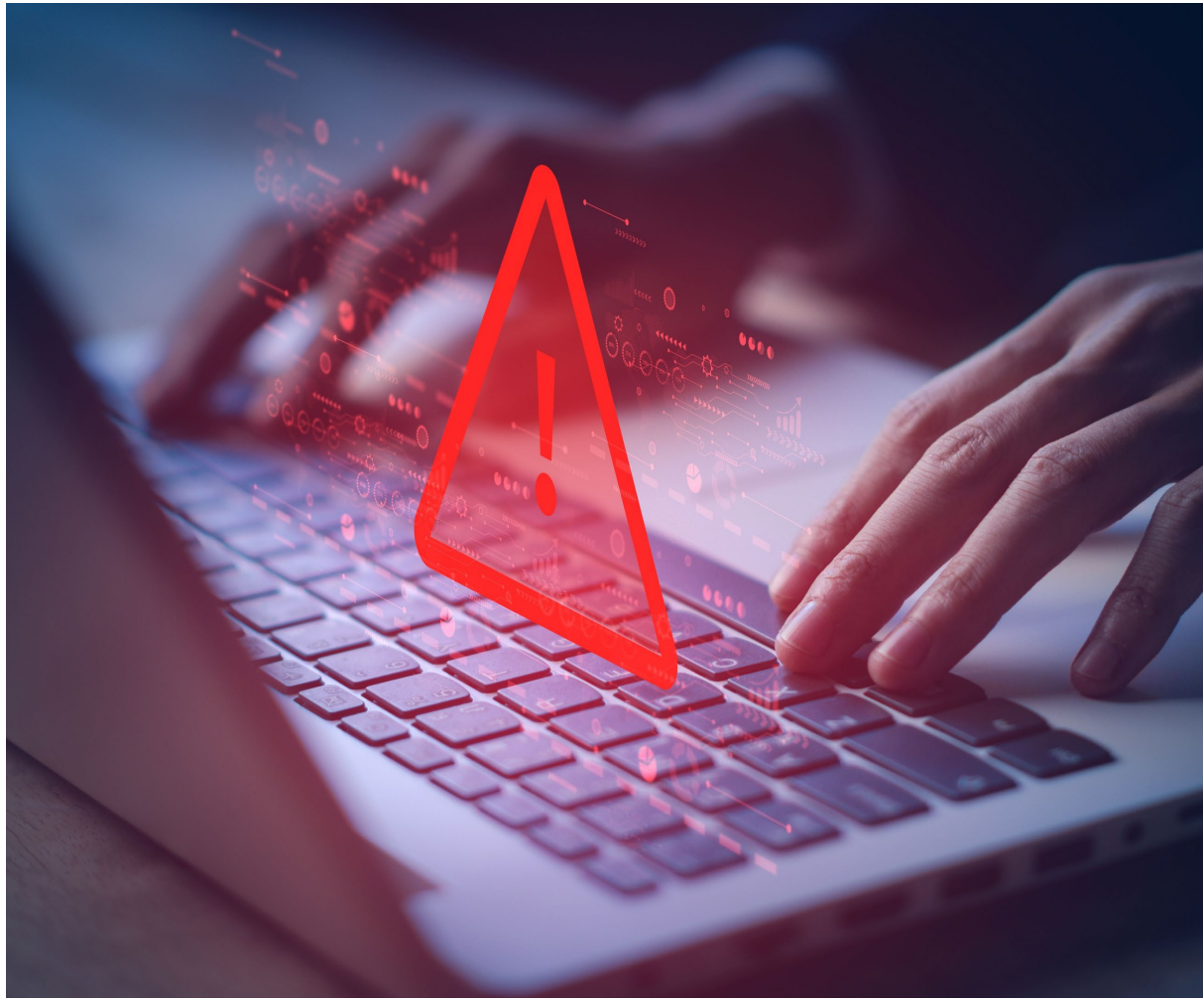
- Microsoft 365
- Fuel Management (e.g. i6 Fusion6)
- JIG Dashboard
- Airline Operator Training Portals
- ID Verification Gateways
- Time & Attendance
- HR Portal

Operational Technology

- PLCs
- HMI Interfaces
- Historian Server(s)
- Automatic Tank Gauging
- 4G Modems
- Electronic Water Sensors
- Hydrant Pit Valves
- Valve Actuators (e.g. Rotork)
- Additive Injection System
- Bowser Telematics
- CCTV
- IR Fire Protection

VULNERABILITIES – EXPLOITABLE SECURITY WEAKNESSES

- Lack of regular security awareness training
- Missing security updates on laptops
- Legacy hardware
- Ineffective Anti-Virus software
- Weak passwords
- Lack of Multi-Factor Authentication (MFA)
- Weak supplier management processes
- Poor network segregation
- Inadequate data backup processes



THREAT ACTORS – THE BAD GUYS

Motivation - The underlying reason a threat actor wants to attack.

Example: A hostile state seeking to steal aircraft or engine design IP for strategic and economic advantage.

Intent - The actor's desire and determination to act against a specific target, what they actually aim to do and how committed they are to doing it.

Example: A cyberterrorist group deliberately choosing an airport as a target with the clear aim of causing disruption and public fear.

Capability - The actor's actual ability to carry out the attack: their skills, resources, tools, and access.

AVIATION THREAT ACTORS - KNOW YOUR ENEMY

- Nation State Actors (APTs)
- Organised Criminal Gangs
- Cyberterrorists
- Malicious or Negligent Insiders
- Supply Chain Attackers

KNOW YOUR ENEMY – NATION STATE ACTORS (APT)

State-sponsored and well-resourced - Backed by government funding, intelligence services, or military, giving them access to budgets, tooling, and personnel far beyond ordinary attackers.

Highly sophisticated - Capable of developing custom malware and chaining advanced techniques, including zero-day exploits (previously unknown vulnerabilities) that most defenders cannot anticipate.

Patient and persistent (APT behaviour) - Operate as Advanced Persistent Threats, willing to stay hidden inside a network for months or years, conducting slow, low-profile operations to maintain long-term access.

Strategically motivated - Driven by geopolitical, military, or economic objectives rather than quick profit - typically espionage, intellectual property theft, or pre-positioning to disrupt critical infrastructure if needed.

KNOW YOUR ENEMY – ORGANISED CRIMINAL GANGS

Financially motivated - Driven almost entirely by profit, through ransomware, fraud, data theft, and extortion, rather than ideology or espionage.

Run like a business - Operate as structured, professional enterprises with specialised roles, affiliate models, and even "as-a-service" offerings (e.g. Ransomware-as-a-Service) that lower the barrier for others to attack.

Capable but cost-conscious - Skilled and well-organised, but tend to favour proven, scalable techniques (phishing, stolen credentials, known vulnerabilities) and go after targets offering the best return for least effort.

Opportunistic and high-volume - Often cast a wide net across many organisations, prioritising those that are poorly defended or where disruption makes a quick payout more likely.

KNOW YOUR ENEMY – CYBERTERRORISTS

Ideologically motivated - Driven by political, religious, or extremist causes rather than profit, seeking to advance an agenda or make a statement.

Aim to cause fear and disruption - Goal is to intimidate, destabilise, or cause physical-world harm, targeting safety-critical and operational systems for maximum impact rather than data or money.

Drawn to high-profile, symbolic targets - Deliberately choose visible, critical infrastructure (such as aviation) where an attack generates publicity, public fear, and media attention.

Variable capability, high intent - Skill levels range widely from low-resource groups to those with state backing, but they are defined by a strong willingness to cause damage regardless of consequences.

KNOW YOUR ENEMY – MALICIOUS (OR NEGLIGENT) INSIDERS

Hold legitimate, trusted access - Employees, contractors, or partners (flight crew, ground handling, maintenance/MRO, IT, baggage and cargo staff) who already have authorised access to systems and facilities, so their activity often looks normal.

Varied motivations - Often driven by financial gain, revenge over grievances, ideology, or coercion. Can be recruited or bribed by external groups (including organised crime or hostile states) seeking an insider foothold.

Hard to detect, high potential impact - Bypass perimeter defences from the inside, they can cause serious harm before discovery.

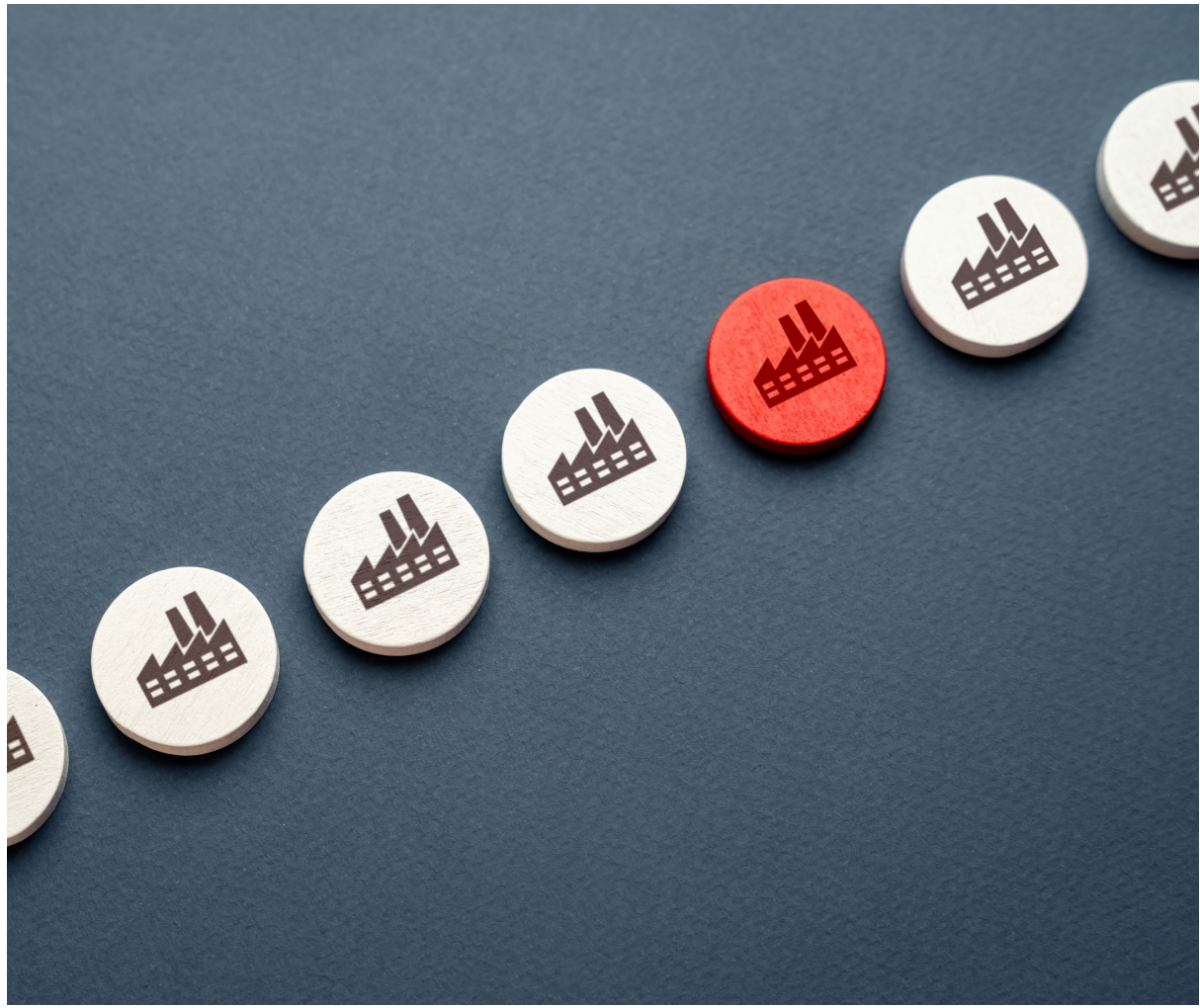
Exploit deep operational knowledge - They understand internal processes, controls, and weak points, such as which systems lack monitoring or how procedures can be bypassed.

KNOW YOUR ENEMY – SUPPLY CHAIN ATTACKS

Target trusted third parties - Rather than attacking the airline or airport directly, they compromise a trusted supplier (avionics and software vendors, parts manufacturers) and use it as the path into the real target.

Exploit a large, interconnected ecosystem - Aviation depends on an exceptionally broad and deeply integrated vendor network, so a single compromised supplier can ripple across many operators at once.

Hard to detect through trusted channels - Malicious code or access arrives via legitimate software updates, components, or established connections, so it bypasses defences and looks like normal, authorised activity.



THREAT ACTORS - AVIATION IS A CONSTANT TARGET IN 2026

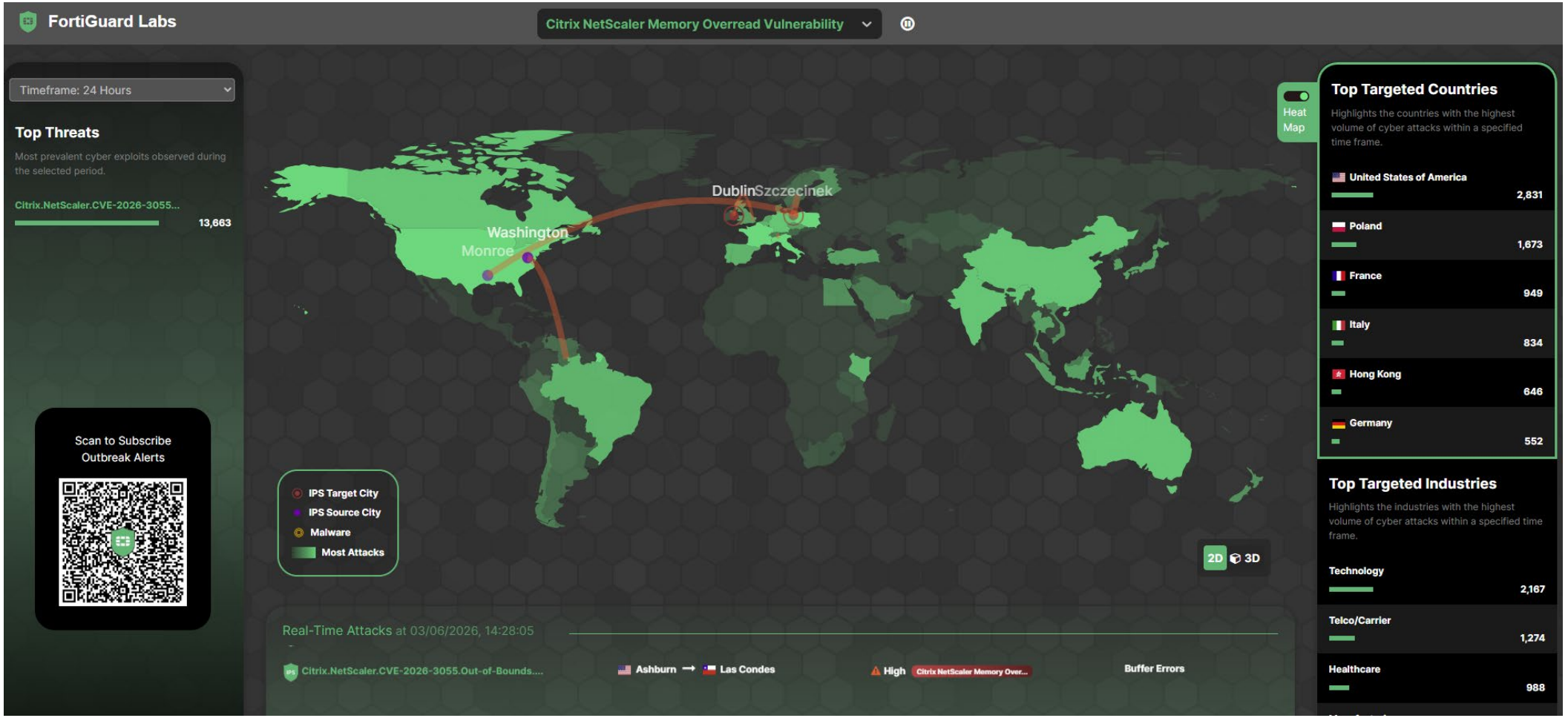
Hazel Sandstorm (Origin: Iran)

- Hacking Group linked to Iran's Ministry of Intelligence and Security (MOIS)
- Targets airlines, telecommunications, utilities, oil & gas companies
- Uses phishing attacks to gain initial access to airline networks, then installs custom malware to maintain access

Tumbleweed Typhoon (THORIUM) (Origin: China)

- Active since 2018
- Targets Airlines & Aviation Service companies
- Compromise web services & VPNs to gain access
- Install Command & Control (C2) malware to exfiltrate sensitive data and maintain access to organisation

THREAT MAP



https://fortiguard.fortinet.com/threat-map

IMPACT

Confidentiality - Ensures sensitive data is accessed only by authorised individuals. The Principle of Least Privilege (PoLP) should apply through strong Role-Based Access Controls (RBAC).

Integrity - Guarantees data accuracy and reliability by preventing unauthorised modification, often using hashing and digital signatures.

Availability - Guarantees that systems and data are accessible when needed.

IMPACT TO AVIATION FUELLING COMPANIES

- Major fuel delivery outage at the airport. May only be able to operate manually for a short period of time. **(Impact: Availability)**

- Exposure of commercially-sensitive information (e.g. airline fuel consumption, fuel purchase prices etc). **(Impact: Confidentiality)**

- Malicious modification of fuel sample data **(Impact: Integrity)**

LIKELIHOOD

- Likelihood is the probability a threat will successfully exploit a vulnerability and cause harm.
- Likelihood rises with capable, motivated actors and exposed weaknesses, and falls with strong defences, monitoring, and good security hygiene.
- High-value, high-profile sectors such as aviation face a higher baseline likelihood simply because they draw more attacker interest.

CYBER RISK SCORING

- Risk scoring is conducted to calculate the Inherent & Residual Risk
- **Inherent Risk** – The level of risk without any controls applied
- **Residual Risk** – The remaining level of risk once risk treatment has been applied
- Usually, a 5x5 risk matrix is used, which is similar to safety or operational risk scoring
- Risk Acceptance Criteria is defined to indicate the organisation's risk appetite. For example: **Low**
- The Residual Risk must be within the Risk Acceptance Criteria

	Negligible	Minor	Moderate	Significant	Severe
Very likely	Low - Medium	Medium	Medium - High	High	High
Likely	Low	Low - Medium	Medium	Medium - High	High
Possible	Low	Low - Medium	Medium	Medium - High	Medium - High
Unlikely	Low	Low - Medium	Low - Medium	Medium	Medium - High
Very unlikely	Low	Low	Low - Medium	Medium	Medium

CYBER RISK TREATMENT

CYBER RISK TREATMENT

1. Unsupported Windows 10 Operating System (OS).

1. Migrate to Windows 11; isolate and patch legacy devices.

1. Legacy devices remain; however, these are isolated.

CYBER RISK TREATMENT

Inherent Risk

1. Unsupported Windows 10 Operating System (OS).
2. Lack of MFA means stolen passwords give account access.

Risk Control

1. Migrate to Windows 11; isolate and patch legacy devices.
2. Enforce MFA on all accounts using phishing-resistant methods.

Residual Risk

1. Legacy devices remain; however, these are isolated.
2. Takeover unlikely but some social engineering risk remains.

CYBER RISK TREATMENT

1. Unsupported Windows 10 Operating System (OS).
2. Lack of MFA means stolen passwords give account access.
3. Unmanaged devices in use with unknown patching, encryption, and security posture.

1. Migrate to Windows 11; isolate and patch legacy devices.
2. Enforce MFA on all accounts using phishing-resistant methods.
3. Enrol in MDM; enforce baseline; block non-compliant devices.

1. Legacy devices remain; however, these are isolated.
2. Takeover unlikely but some social engineering risk remains.
3. Devices meet baseline. New or guest devices are blocked.

CYBER RISK ASSESSMENT SERVICE

- Identify the level of risk that is associated with your organisation's information assets through a threat & risk workshop, with a management report and cyber risk register provided at the end.

- Cyber Risk Assessments align with many regulatory requirements, like NCSC Cyber Assessment Framework, NIS2, IEC62443 & EASA Part-IS.

- Previously, we've conducted Cyber Risk Assessments for several JIG members, which now form part of their organisation's risk register.

PAPER, PAPER AND EVEN MORE PAPER !

- One fuelling organisation had a total of **12 unlocked filing cabinets** full of potentially sensitive and business critical information.

- Information included Into-Plane Transfer Receipts, Maintenance Logs, Fuel Quality Reports and Operating Manuals.

- Risk of critical information being lost or destroyed with a significant operational impact.

- Digitisation projects are strongly recommended.

LACK OF MULTI-FACTOR AUTHENTICATION (MFA)

- Business critical applications in fuelling organisations are sometimes secured with a simple username and password.
- Operator Training or ID Verification Portals contain sensitive personal information (e.g. passport scans), which in some cases, can be accessed without MFA.
- Implement Multi-Factor Authentication (MFA) or Single Sign-On (SSO) if possible.
- Petition Operators to improve portal security.

UNMANAGED LAPTOPS IN USE

- Unmanaged laptops (sometimes personally owned) were being used to access company information.

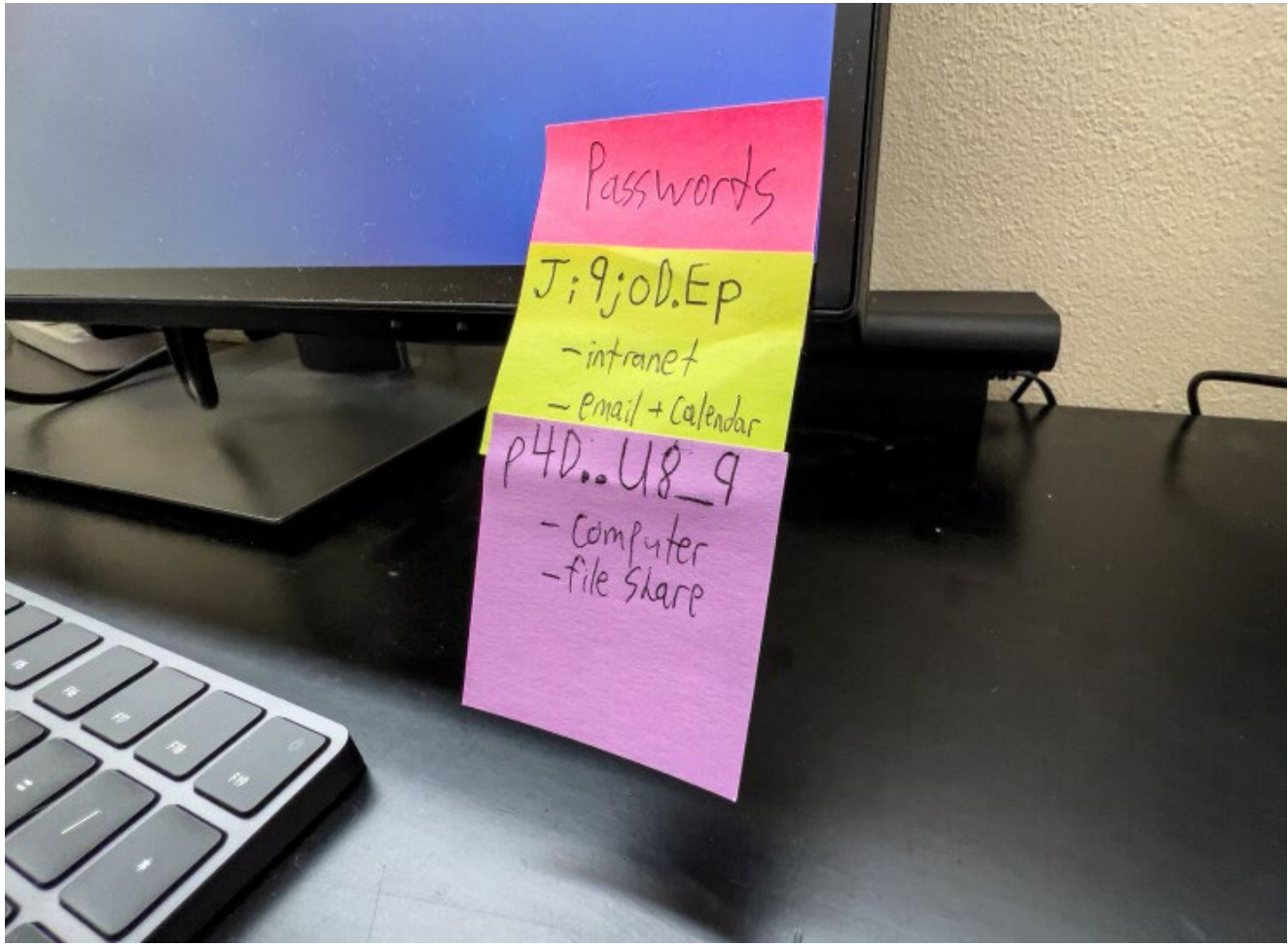
- Faudi Electronic Water Sensors (EWS) and other data collection systems need USB access which was blocked on company laptops.

- Significant security risk as these devices may not meet the organisation’s security baseline for patching, encryption, malware protection, or device configuration.

- Sensitive organisational data could potentially be exposed.

PASSWORDS WRITTEN ON POST-IT NOTES

- Credentials for business-critical applications were written on Post-It notes and fixed onto monitors in the staff break room.
- Generic accounts or credential sharing is very common across aviation sector.
- Sharing credentials prevents a robust audit trail from being maintained for user access.



LACK OF VULNERABILITY MANAGEMENT

- Lack of regular vulnerability assessments and annual penetration testing
- Large number of aviation fuelling customers had never conducted any form of penetration test of their network or applications !
- Assumption that a 3rd party is looking after the vulnerability management or that Automatic Updates will stop their devices from being compromised

FINAL APPROACH

- Cyber risks in the aviation sector often have real-world physical consequences, which can directly affect fuelling operations and passenger safety.

- Cyber risks should be assessed and present on your organisation's risk register and regularly reviewed by your management team or a 3rd party.

- Reducing the level of Cyber Risk in your organisation should be led from board level but it is everyone's responsibility.

SecureTeam

QUESTIONS