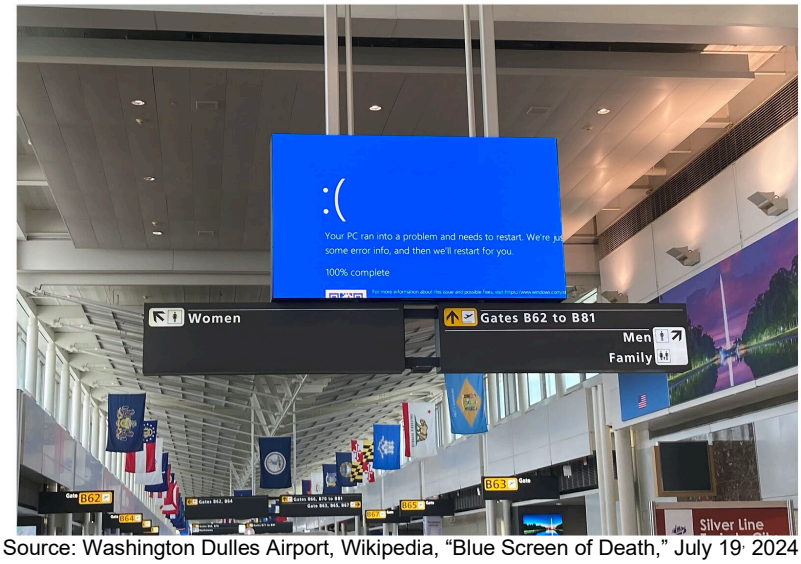
Global IT Outage - Airline Industry: Cyber and Turbulence Risk



Source: Washington Dulles Airport, Wikipedia, "Blue Screen of Death," July 19, 2024

Synopsis

"No plan survives first contact with the enemy."— Helmuth von Moltke [i]

On July 19, 2024, a respected cybersecurity company distributed a faulty update to their security software, causing widespread problems with computers running the software. The global impact was that 8.5 million systems became functionally inoperable, in what was called by cybersecurity expert Troy Hunt, "the largest outage in the history of information technology."[ii] The extent of this manmade catastrophe is recorded in Wikipedia, [iii] with the airline industry taking a lot of the impact.

Initial estimates of economic damage are $10 billion to $15 billion, with insurance losses around $1.5 billion [iv]. This was not a cyberattack or malicious act, but human error, which according to the World Economic Forum accounts for 95 percent of cyber incidents today [v] and is preventable by ensuring data and cyber integrity by design.

Although a fix was created within 30 minutes of the incident, the risk had become systemic; the misconfiguration error addressed an operating system kernel, which detects cyberthreat

vulnerabilities at the organizational endpoints (user devices) for which frequent fixes (patches) are distributed by the cybersecurity company. Once deployed, the devices did not reboot and showed a “blue screen of death.” [vi]3. This meant IT staff had to go to physical locations to reboot servers and apply the fix manually in old school fashion.

The incident sparked the aggregation fears of the insurance industry as 50 percent to 60 percent of the Fortune 1000 companies were all using the same company cybersecurity software [vii]. Downward counterfactual thinking tells us that this incident could have been much worse, as only 1 percent of all Windows devices were impacted, according to Microsoft [viii] . In relative catastrophe terms, this incident, although widespread, could be considered a “near miss,” unlikely to affect the insurance industry in the short term. However, steps need to be taken to better mitigate future scenarios to reduce the risk of such an incident happening again, especially if instigated by malicious actors, where the outcome could have been severe.

The global airline sector was the most affected, with business interruption stemming from cancelled flights, crew tracking, backlog, cargo issues, and passenger disruption, with failure of client software platforms displaying the blue screen of death in the airports. All business sectors were affected on a global scale including banks, hospitals, rail transport, media, telecommunications, and retail, with the maritime ports being less affected.

The incident created openings for malicious actors during the confusion, leading to potential national security issues. This refocuses attention on airline sector risk management after the turbulence event of May 21, 2024. [ix] Turbulence requires airlines to use new apps and technology, which need to be protected assets in the cybersecurity and vulnerability space.

Definitions

- **Blue screen of death (BSOD):** A reference to the colour of a user's system screen after a fatal Windows system error. The screen turns blue with white text, providing a message that the system is largely inoperable from a functional perspective.
- **Browser plug-in:** Software designed to manage internet content outside what the browser was designed to perform; can be a high cyberattack vector.
- **Causal (AI) reasoning:** Technology that can reason and make choices like humans. It utilizes causality to extend beyond narrow machine learning predictions and can be directly augmented with human decision making.
- **Chief information security officer (CISO):** A person implementing cybersecurity.
- **Common vulnerabilities and exposures** (**CVE**): A database of publicly disclosed information security issues. A CVE number uniquely identifies vulnerabilities from the list.
- **Configuration management database (CMDB):** A database used by an organization to store information about critical hardware and software assets; acts as a data warehouse for an organization, storing information and metadata regarding the upstream and downstream relationships of the assets.
- **Downward counterfactual thinking:** [x] A mental simulation on how an event could have been worse to put what has occurred in a more positive light. This has not been systematically utilised to date for regulatory efficiency or mitigation purposes.
- **Endpoint security:** The process of protecting devices like mobile phones, laptops, and sensors from malicious threats and cyberattacks.

- **Mean time to patch:** A metric that tracks the average time an organization applies patches to vulnerabilities, software bugs, or other security issues. Timely patching is paramount in cybersecurity: if critical vulnerabilities remain unpatched for extended periods, it increases the risk of exploitation by malicious actors.
- **Multi-factor authentication (MFA):** A multistep security login process requiring more than a password, often involving biometrics.
- **Patch management:** A process of applying vendor-issued updates to close known exploited vulnerabilities in software and devices.
- **Security orchestration:** This allows the sharing of information by automation, enabling multiple tools to respond to incidents as a group, even when the data is spread across a large network and multiple systems or devices.
- **Service level agreements (SLA):** A contract between a company and service provider.
- **Vulnerability:** A weakness in an IT system that can be exploited by an attacker to deliver a successful cyberattack. They can occur through flaws, features, or user error. These are system bugs and coding errors fixed by patching.
- **Zero-day exploit:** A cyberattack vector that takes advantage of an unknown or unaddressed security flaw in computer software, hardware, or firmware. "Zero-day" refers to the fact that the software or device vendor has zero days to fix the flaw because malicious actors can already use it to access vulnerable systems.

Overview

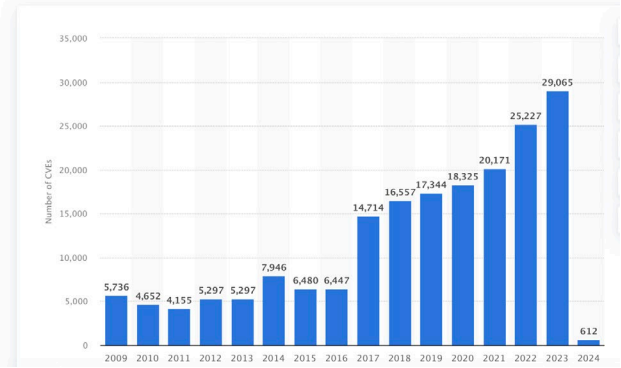
While it was a wake-up call for all organizations, the IT outage incident was not unforeseen, tinged with an element of surprise for cybersecurity experts as to the cause. Mitigation of vulnerability current practice is now under the microscope and insurers will be updating their risk assessment accordingly.

This is likely to be in the form of endorsing a risk-based approach to cyber vulnerability management where each vulnerability is evaluated as a peril, based on exploitability, business impact, and exposure. It will direct the way patch management is done, creating stability by testing patches in a controlled way (no direct patching into production) with rollback plans, leveraging automation where possible to reduce human error but keeping humans in the loop using causal AI reasoning [xi] and orchestration to deploy large-scale patch management. This avoids a strategy of “patch at all costs,” limiting patching to critical vulnerabilities exploited in cyberspace and using risk-based prioritization and “patch on demand.”

Non-critical patching can be delayed without risk, which will also foster collaboration between IT and cybersecurity teams with shared metrics, reporting and educating stakeholders on patching culture. This continuous journey of feedback loops and post-patch analysis is vital given the statistics for cyberthreat emerging in 2024. [xii]

According to recent podcasts, it takes 58 days to remediate internet-facing vulnerabilities.[xiii] The total damage caused by cyberattacks in 2022 was $8.4 trillion, which is expected to rise to $23.84 trillion by 2027 [xiv]. Every 39 seconds in 2023, there was a cyberattack, [xv] with ransomware attacks happening every 14 seconds [xvi]. Unpatched vulnerabilities are the target of 95 percent of all cyberattacks [xvii]. The number of common vulnerabilities increases each year,

as illustrated in the following graph by Statitica [xviii] showing the number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD.



Source: Statitica

The cybersecurity company involved in the outage is an endpoint security service using cloud computing to apply cyber detection patches to devices connected to the internet. These patches can also be applied directly to backend systems on premises. With many companies becoming cloud first, which prioritizes cloud over on premises, there must be trusted cloud in this era of digital sovereignty.

Cloud is “somebody else’s computer.” This simple truth is the root of the data sovereignty, security, and trust problems that previously hampered the adoption of cloud by the public sector and critical regulated sectors. However, cloud is the future for cost savings, efficiency, greener computing, and business process innovation, as users can outsource IT infrastructure and focus on core businesses.

As well as sharing the same risks as on premises, new approaches need to be taken for cloud cybersecurity using digital twin technology [xix] to track, in real time, the state of any process or data in the cloud. This makes it possible to trust and verify everything that is happening in a cloud deployment and solves the “somebody else’s computer” problem. Cloud provides the infrastructure for processing data at volume, providing convenient, user-friendly services, or adopting new technologies such as artificial intelligence (AI), 5G, and edge computing. This allows small organizations to scale up operations quickly and gives larger organizations a competitive advantage. Among the Fortune 1000, cloud adoption is now recognised as reaching near universal acceptance.

Mitigation of Future Outages

A risk-based framework managing vulnerability and robust remediation strategy using a preventative and predictive approach is required to control the software, hardware, and data assets on a network. There must be actionable, data-driven strategies on patch management, a critical practice that is time-consuming and error-prone in large organizations.

Source: cyvatar. [xx]

Software solutions can automate these tasks, making the process more efficient and reliable. A misconfigured patch is worse than the problem itself, and things can go wrong as they did on July 19, causing a security incident with the same impact as a supply-chain cyberattack. There was no malicious intent as a trusted communications channel sent a misconfigured update patch directly into the heart (kernel) of computer server operating systems.

The vendor determined the problem and devised a fix within 30 minutes, but the computers could not reboot automatically; IT staff had to physically go around to each computer to remediate, some in remote locations. This serious outage impacted millions and was preventable, as all patches can be compared to compliance standards prior to implementation and prevented from being applied if faulty.

Many vulnerabilities and misconfigurations are being discovered daily, overwhelming IT teams, but IT and cyber teams need to prioritize what needs to be patched first; they must align the business with the cybersecurity and the IT. What matters most in cybersecurity is fixing high-risk priorities on time to keep the business safe and protect the brand reputation.

Source: Centre for Internet Security (CIS) [xxi]

The sheer scale of the vulnerability problem increases when it includes misconfigurations. These vulnerabilities can go unnoticed for months and be exploited by malicious actors at any time as the period between infection and discovery can be many days. While the use of zero-day exploits is on the rise, Mandiant's M-Trends 2024 report [xxii] reveals improvement in global cybersecurity posture, showing the global median dwell time (the time attackers remain undetected within a target environment) has reached its lowest point in over a decade.

However, according to the Cybersecurity and Infrastructure Security Agency (CISA)'s Known Exploited Vulnerabilities (KEV) Catalog, 85 percent of vulnerabilities still remained un-remediated [xxiii] after 30 days, with a sliding scale of 55 days (50 percent), 180 days (20

percent), and 365 days (8 percent), requiring a change in security posture, mean time to patch, and risk prioritization.

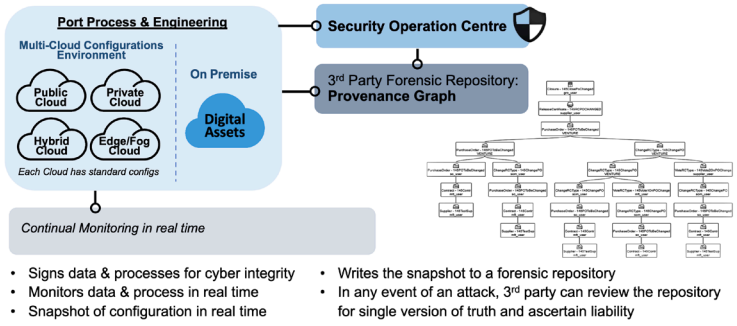
Cybersecurity patch management reduces the risk of cyberattacks by ensuring reliability of systems and balancing security risk with operational risk so that delaying non-critical patches does not cause security incidents. Patching more vulnerabilities increases the operational risk, but this can be mitigated by deploying the minimal number of patches by prioritization. Devices can be removed from the chain of attack by permissions without applying patches. If the device cannot be mitigated and there is a high risk of exploitable vulnerability, then the device can be isolated from the network until the issue is resolved.

Zero-day exploit scenarios, by definition, do not have a patch, so workaround fixes are deployed on the assets so the attackers cannot exploit until a patch is received, which may involve rollback of the workaround. Vulnerability discovery and asset inventory is used to understand exposure in these zero-day scenarios, which require critical attention.

An important area which also needs attention is the configuration management database (CMDB), with a need to improve cyber asset management capabilities. Often the hardware and software assets in the CMDB are not up to date and data assets are absent.

The risk-based approach utilizes threat intelligence analytics and modeling to define the elements of preventative capability by aligning with the exploitability of underlying systems. That leads to maintaining data and cyber integrity of the underlying processes and data assets through patch management.

This is a holistic approach leading to the remediation of the exposures and protecting sensitive data. Automated patching can streamline and reduce human error to minimize disruption across hybrid, on premises, and cloud infrastructure, then monitor and operationalize continuously. Provenance graphs from embedded blockchain use are utilized to non-repudiate what has happened and ascertain liability, as shown below.

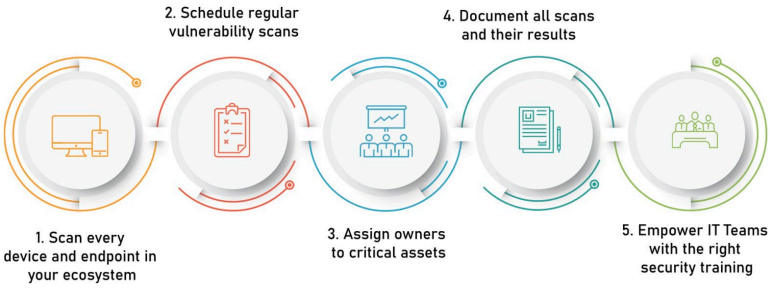


Source: Cymar [xxiv]

Endpoint Management

Large organizations need to ensure the cyber hygiene of endpoints and patch thousands of endpoint devices attached to multiple servers and remediate the vulnerabilities at scale, especially with a travelling or remote workforce. Verizon adopted machine state integrity (MSI) [xxv] to address these issues. Data and reputation of the company must be protected with zero vulnerability and continuous monitoring, requiring a move to cloud computing and a reliance on robust CMDB-based asset management to enable analytics by using scanning tools to quantify the risk. Endpoints are monitored and remediated from noncompliance by using software whitelists to ensure user download of the latest version. A decision needs to be made on embedding generative AI within the products as a potential emerging cyber risk.

Many organizations have no visibility into many of their assets with gaps in asset inventory coverage, especially around data assets. Organizations are using scanning tools to correct this CMDB issue, both from a vulnerability standpoint, such as Qualys [xxvi], and pulling structured/unstructured data from third-party sources to find and quantify missing data asset records such as SyberGRC [xxvii]. This creates a new approach to cybersecurity asset management, with expanded discovery and cyber risk assessment based on risk scores that can be used in insurance underwriting. It can detect unmanaged devices in real time and correlate data assets to isolate threats on the external attack surface, reducing false positives and focusing on unknown vulnerabilities.



Source: Spiceworks [xxviii]

Because of the changing cyber landscape, there is an issue with tool-smithing in the large-enterprise security operation centres (SOC) operations functioning in a highly regulated space. Bad actors have enough resources to exercise significant damage. Underreported business email compromise at 1.8 billion [xxix] is an underestimated peril and not frequently modeled by insurance. Data theft losses now stand at $1 trillion in total [xxx].

Data should be collected to assess the risk of compromise in environment. This would include security logs from all workstations, servers, mobile devices, and third-party security products; software no longer vendor supported; browser history; and extensions from every machine, including all open ports, to get a complete app inventory. Visibility is needed to every running process, especially things like PowerShell [xxxi] script files used to automate IT functions.

Browser plug-ins [xxxii] can conceal malware extensions to perform crypto-jacking and steal financial information. Because this data is hard to collect, the chances of compromise increase significantly if best practices are not applied. Browser plug-ins have permissions, talk to the

internet, read history and identity in email, and access enterprise attributes. An inventory of these is needed to show where they are installed and where they are updated, such as Adobe Acrobat to view pdf files in the browser and Java development platforms.

Cloud Computing Mitigation

Cloud services require trust in the cloud service provider (CSP) for data security and integrity. CSPs do not always give you all the levers you need to understand and manage the security (confidentiality and integrity) of your data and processes. Cloud services have unique security vulnerabilities and have the same security issues as on-premises IT services.

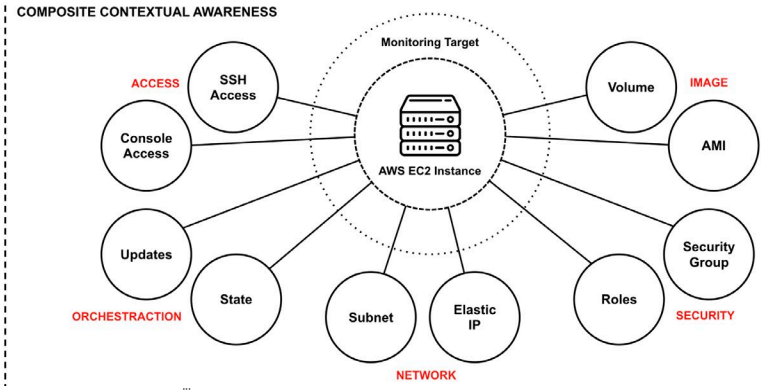
Major cloud services pose an attractive target for attackers as a security exploit can give global access to many high-value customers. Even when cloud services are secure, misconfiguration and administrative errors frequently create security holes. With the growing complexity and virtualization of cloud architectures, this trend will increase.

Over the last decade, the paradigm for cybersecurity has been largely perimeter control, with signature-based heuristics and AI probabilistically making assertions of potential compromise. This approach breaks down in the cloud era as edge/IoT services are running on someone else's infrastructure, so there is no perimeter to protect.

Security and audit costs are high in the log ingestion and analysis space. Vendors often charge by the number of logs stored, which means escalating costs with growing data volumes. Log analysis cannot be fully automated and breaches are detected weeks after they occur.

Regulators have supported new cloud security standards and certifications, but these are box-checking exercises confirming compliance of a cloud service at point of audit, but not ongoing compliance for services constantly renewing and updating.

The following shows complete situational awareness of cloud security with continuous monitoring and orchestration.



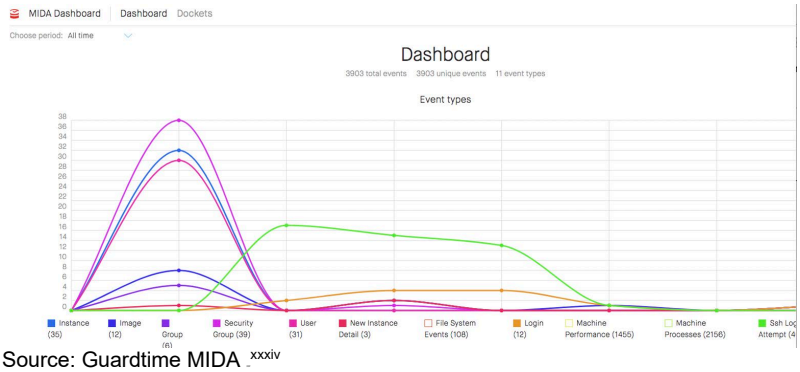
Source: Guardtime [xxxiii]

New approaches are required around securing digital assets, delivering real-time, byte-by-byte-level information of what is happening in a cloud service, thereby

controlling cloud and edge computing. This means verifying the integrity of security control policies and the actual state of data, infrastructure, and services in real time, reflecting the reality of the infrastructure across cloud environments.

Every digital asset on the network (virtual machine, firewall rules, event data, configuration files, etc.) is assigned an immutable digital twin done at scale using blockchain technology, providing a mathematical proof of correctness. Any change in the environment away from the policy generates a high-quality alert that can be remediated in real time, closing the loop between policy and infrastructure and giving rise to a cryptographically enforceable policy. With this approach, real-time breach detection, fast incident response, and dynamic attestation of compliance for external auditors become possible, addressing the ephemeral nature of cloud, where machines and services are quickly used, consumed, and deleted.

This also protects against cloud-specific vulnerabilities, allowing for automated remediation and incident response (e.g., sandboxing, blacklist, deprovision, induce access lag, and rollback to a last known good state). This decreases time to detection as breaches and changes are detected in real time using a dashboard and addresses insider threat protection as malicious insiders cannot alter or exfiltrate data without detection and alert. The benefit is decreased operational costs, decreased storage costs for logs and files, automated event detection and alerting, reduced staffing requirements, and cost-effective device and machine management. The use of dashboards to ringfence all these events is used, as shown below.



Source: Guardtime MIDA [xxxiv]

Configurations must be trusted to make sure the cloud is arranged in compliance with predefined control templates (National Institute of Standards and Technology [NIST] cloud standards [xxxv]), catching both human errors and attempts to alter permissions and configurations by malicious breach. Snapshots are made across the cloud at regular intervals and hash key evidence placed in a repository to share incident information in real time with regulators, forensics, auditors, and other third parties in a granular manner without exposing sensitive information. This enables global outage mitigation and prevent misconfigurations.

This creates a holistic single picture across the enterprise. As new assets are subscribed, they are automatically enrolled into the existing monitoring program, pulling together security information across multiple cloud services, agencies, and deployments into a “single pane of glass.”

The primary cloud threats are misconfiguration, misuses of common credentials, or accidental asset creation. Adaptive state capture and event correlation allows cloud owners and operators

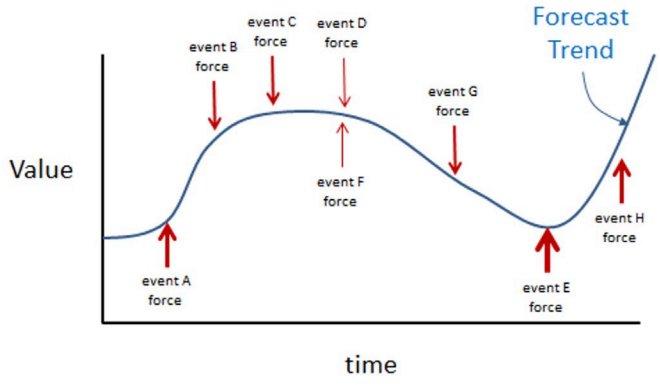
to significantly reduce the time from accidental or malicious event to remediation. This cryptographically "containerizes" the systemic state of the cloud using snapshots which leverage the blockchain to enforce accountability, immutability, and time of creation. The snapshots contain the various types of state and seal them into a token, making them portable and durable for event correlation and analysis with long-term storage.

Use of Causal AI Reasoning for Predictive Cyber Risk Management

Traditional AI and machine learning (ML) are used in cybersecurity to find attack trends and patterns in large datasets at speed. Correlation-based machine learning has limitations due to spurious correlations, so there has been an inability to accurately predict future attacks and adapt to a changing threat landscape. Causal (AI) reasoning is a better approach for the SOC to detect and uncover potential threats and create predictive models.

Correlations are inadequate at predicting the future as they do not imply causality.[xxxvi] Causal reasoning overcomes these issues by leveraging advanced machine learning algorithms to understand and analyse root cause-and-effect relationships within complex systems. It will endow and make a significant impact on existing AI/ML systems. The causal AI market was $8 million in 2023 and expected to grow to $120 million by 2030 .[xxxvii]. In the context of cybersecurity, it plays a crucial role in identifying the underlying causes of cyberthreats and attacks, enabling organizations to develop proactive defence strategies.

Increased computational power amplifies the potential of causal AI for cybersecurity. By analysing vast amounts of data and identifying causal relationships, a deeper understanding is reached about how cyberthreats originate and spread. This allows identification of vulnerabilities and potential attack vectors, leading to more effective threat detection and prevention measures using predictive analytics by shaping outcomes on the impact of different security controls and measures on overall cybersecurity posture. Feature sets are created with chief information security officers (CISOs) and threat intelligence to create causal models. These models are then used to create hypotheses that can be validated to test the accuracy of the predictions by back testing with historical observations.



Source: Vulcain.AI

In the diagram from Vulcain.AI [xxxviii], a baseline moves through time and is impacted by cyber events. Events A, F, E, and H apply upward forces, causing the value of the forecast trend to increase over time. These forces would be, for example, past cyberattacks, such as NotPetya [xxxix], Wannacry [xl], SolarWinds [xli], and the recent outage event. Events B, C, D, and G are applying downward forces, causing the value of the forecast trend to decrease over time; these would be the mitigation success metrics, reduced dwell time, zero-day exploit suppression, and so on.

The magnitude of the event forces is indicated by size of their respective arrows. If these forces are known, the value of the forecast trend can be determined at any point in time and predicted for future periods, thus improving threat detection. A message should go to its destination directly; but if it is detected that it went a circuitous route, then likely there is a root cause cyberattack. This approach can prevent zero-day exploits from entering systems, creating a preventative approach, and the attackers will be unable to detect the causal algorithms.

Causal reasoning helps cybersecurity systems to better understand the causal relationships between cyber events and identify potential threats and vulnerabilities before they escalate, allowing for proactive threat mitigation while r**emoving bias and ambiguity caused by correlation and confounding variables.**[xlii] **This reduces or eliminates false positives or spurious correlations that occur with traditional AI systems.** By identifying the causal factors behind security incidents and understanding which components are most critical to the organization's operations, it can help prioritize cybersecurity resource allocation.

Finally, causal AI adapts to the changing threat landscape by testing hypotheses on how changes in the network or system may affect cybersecurity and adjust accordingly to stay ahead of evolving threats shaping future outcomes positively before they occur.

Turning Cybersecurity into a Profit Centre

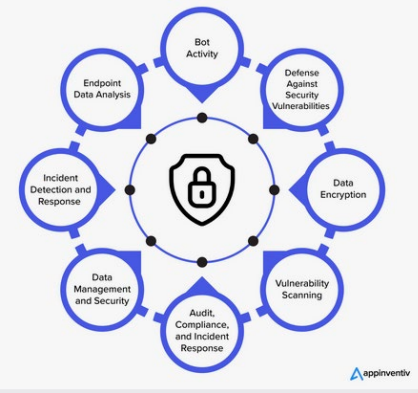
Boards of directors in general do not understand the return on investment for cybersecurity, especially data integrity, so there is a need to emphasize the importance of vulnerability management and impact on the business. People have short memories, and this global outage is a wake-up call, showing misconfigurations can seriously hinder business operations.

Moving to a risk-based mitigation approach to get buy-in of management is paramount. Reduction of patching only critical issues on demand and using automation to remove the human error element are top-of-mind issues. Nearly all data breaches, going back to the Target event of 2013 [xliii], have been data integrity breaches; but investment in data integrity security has been historically low. It seems that the situational awareness of data as an asset in an organization is still not fully understood.

Zero-day vulnerability exploits may not have a patch released for hours, so automation can reduce the amount of time that a malicious actor can act. The CISO needs to get board approval to leverage virtual security operations centers (vSOCs), [xliv] automated security that can detect and respond via automation, pushing out monthly updates and becoming a team resource and not just a cost center.

If someone clicks a phishing link, this is picked up by vSOC, which is tuned consistently to give real-time threat intelligence with multiple reporting platforms. They understand through

heuristics how networks operate and shut down the bad actors in dark web activities. The following shows the tasks that can be automated.

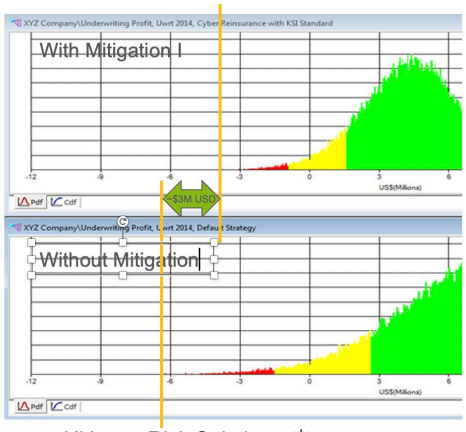


Source: Appinventiv

Security awareness training is vital from top down. It encourages staff to report phishing emails to feed threat intelligence and present these metrics to the board and cyber insurers by using nontechnical language to communicate vulnerability management issues.

The CISO should report to the board as the protector of network and data assets, providing a competitive edge and not being seen as an obstacle to the organization's mission. This in turn will create a profit center, covered by the cost of reducing risk, paying for itself by reduced regulatory fines, stock price increase, customer retention, and lower risk tolerance in operational risk compliance.

The diagram below shows cyber tail risk in red and how this can be reduced in cost terms by mitigation.



Source: Ultimate Risk Solutions [xlv]

Insurance Implications of Outage and Beyond

In the cybersecurity space, continuous monitoring, automation, and vulnerability reduction will have an impact of getting cyber insurance. Following this outage, diversification of security policy against aggregation risk will be enforced. Claims are expected to be submitted to recover business interruption losses; however, the July 19 incident was not a malicious attack, but a security incident caused by human error. The cybersecurity firm accepted liability, but the extent of this will be determined by the terms and conditions agreed with customers in the service level agreements (SLA)s. The disruption of network systems may be covered by property damage and business interruption insurance but after the silent cyber era [xlvi], many businesses have stand-alone cyber policies covering losses from such an outage.

Cyber insurance policies provide coverage for first-party losses (insured) and third-party client liabilities such as network interruptions, data breaches, and ransomware attacks. This outage may trigger both coverages as in addition to incurring losses (plus remediation costs) from system unavailability, there may be liabilities of service to third parties, leading to reputational damage. Time will tell which policies cover network interruption due to non-malicious cyber events at a third-party network service provider. Finally, these policies may have a waiting period of “X hours” or a threshold of loss before the policy is triggered.

CyberCube said insured losses ranged from $400 million to $1.5 billion [xlvii] representing 3 percent to 10 percent of the $15 billion in global cyber premiums held today, although final losses will take time to determine. The outage resembled a supply chain attack, taking out multiple users of the same technology all at once—including airlines, hospitals, banks, stock exchanges, and retail.

Hospitals were disrupted by the outage, with 1 million of the 8.5 million devices affected [xlviii]. Patient operations were cancelled, access restricted to electronic health records (EHR), disruption to machines such as CT scans, MRI machines, X-ray machines, and nursing carts connected to the hospital network, plus connection to on/off-premises pharmacies using electronic prescription scripts.

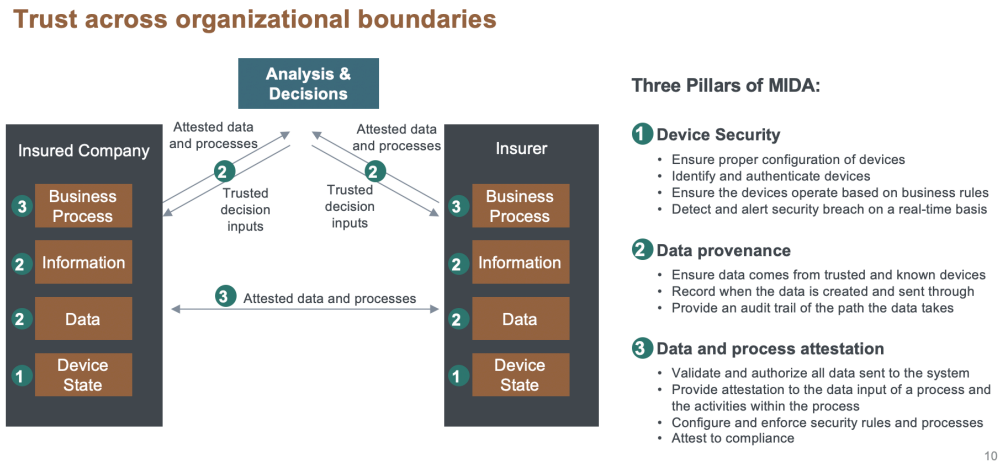
The outage increased the risk of malicious activity on patient EHR to commit identity theft. Unpatched machines could contain software provided by a third party impacted by a vulnerability, allowing an entry point to move laterally across the hospital network to access EHR.

Ransomware is a big concern as a bad actor can encrypt the system, directly affecting the patients. The outage is likely to increase demand for cyber insurance across the board and refine the risk assessment process for vulnerability management, forcing organizations to think, “What if it could have been worse?”

Cyber premiums are rising [xlix] and will increase because of a wider attack surface (AI/cloud adoption), making insurance scarce or premium loaded for many organizations unless they mitigate with proactive risk management. Premium discounts are available for automating vulnerability management, using causal AI for threat intelligence, dark web monitoring, zero trust architecture, identity/access management to networks, plus alignment of IT and security teams.

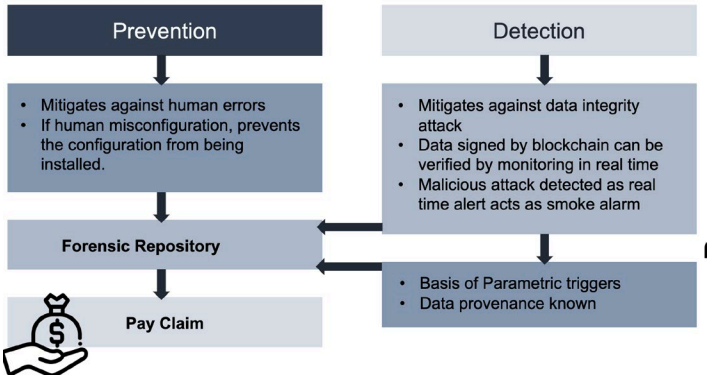
Multi-factor authentication (MFA) is mandatory and moving from SMS to authentication apps [l] will impress underwriters and lead to a decrease in cyber insurance premium. The process must

be data driven and cross organizational boundaries, as shown below, courtesy of Guardtime MIDA [li]. This provides maximum mitigation to non-malicious events.



Source: Guardtime MIDA

For robustness, devices, machines, business processes, and applications must be secure to speed of claims investigation, payments, subrogation, and cross-organizational reconciliation, plus proving policy compliance. Verifiable compliance allows insurers to know the risks their customers are taking leading up to an incident; they rely on this data even if disputed, thus creating provable outcomes. Damage mitigation is obligatory, so insurers must know to what extent the customer mitigated, prevented, and detected in a cyber event.



Source: Cymar.org

Insurers will look to see if risk engineers conduct vulnerability scans of an organization's network and data assets. Insurers partner with policyholders to share threat intelligence around critical vulnerability exploits. This offers risk mitigation incentives to policyholders so if they are deploying new controls or security upgrades, a discount can be made available.

Airline Industry and the IT Outage

Major airlines suffered business interruption losses up to $1 billion at first blush and will pursue damages from the cybersecurity firm involved and maybe Microsoft, as they made heavy use of both technologies [lii]. There will be class-action lawsuits: Delta Airlines alone had to physically reset more than 40,000 servers [liii]. Many of the current SLAs do not hold vendors liable for outages and this could be deemed a foreseeable event that could have been prevented or an unforeseen event covered by insurance.

The use of automation will change the current model, with new guardrails and safeguards to protect the airlines and their passengers as many of the affected systems were passenger information, check-in, and ticketing services. Many airlines grounded flights, with the outage hitting the global supply chain with air freight expecting to take days to recover. This shows how vulnerable marine and air supply chains are to IT outages, hence the criticality of mitigation. This is also a wake-up call for the maritime industry in the compromise of shipping and port digitisation assets, which, while largely unaffected this time, could be far worse next time and should not be ignored.

Commercial airlines and private aviation terminal operators have global fixed-base operations located in multiple countries. They do continuous cyber assessment for aircraft vulnerabilities and threat impact analysis. This means building cyberattack training and awareness into pilot flight simulation, including cockpit intrusion and cabin entertainment system compromise. The endpoint aviation devices all need to be hardened against vulnerabilities.

The CISO must be able to monitor in-air and on-ground operations to secure the network from compliance and from technical standpoints, leveraging third-party partners and automation. For private jets, autopilots need to be cyber managed around the world at global locations and instead of replacing vulnerable machines physically, can mitigate in real time by linking it to the network on a zero-trust model.

Airline Turbulence

The airline industry is affected by both cyber risk and climate risk, when the latter is manifesting itself in the form of turbulence as convective storms increase. Additionally, geopolitical wars are forcing planes to narrower routes, coupled with airlines under pressure to save fuel. A perfect storm could lie ahead as more technology is being applied to address the turbulence risk, which means more assets to protect and mitigate against cyber risk.

From an insurance and risk management perspective, turbulence is an understood risk and covered in travel policies, giving rise to small claims. There does not seem to be specific catastrophe cover for a large event identifying turbulence as a peril, likely through lack of data. Several incidents in May 2024, including death and injuries, and have raised the risk level awareness with events continuing to be recorded in August 2024.[liv]

Turbulence is caused by multiple reasons, but many injuries are from clear air turbulence (CAT) [lv] and technologies are being developed to help aircraft anticipate and avoid CAT. The root cause of recent incidents is not confirmed beyond being “sudden and extreme” as the aircraft entered an area of developing convective storm activity.

Causal AI reasoning can assist in getting to root causes and building a turbulence index. CAT turbulence, which occurs without warning in clear skies at high altitudes, is not easily detectable with conventional onboard weather radar. Pilots read weather conditions in the immediate

vicinity of the aircraft and have access to detailed meteorological weather forecasts. However climate drives weather hence the need to look at root causes longer term.

While weather models provide large-scale information, they do not capture smaller-scale experiences by individual aircraft, so there is a need for a reliable method for detecting CAT in advance. Pilots report it when they encounter it, but locations can be misreported when travelling at more than 500 miles per hour at high altitudes.

Light detection and ranging (LiDAR) [lvi] technologies can reduce CAT risk. The approach works by emitting two laser beams from an aircraft, which receive information about how light is scattered by small dust suspended in the air. LiDAR systems then use the wavelength variations to spot the transitions in airflow that cause turbulence, helping aircraft move around them. NASA [lvii] and the National Center for Atmospheric Research (NCAR) [lviii] are both working on ways to spot CAT, with the latter installing algorithms and monitoring data points on over 1,000 aircraft and correlating with national weather forecasts and prediction models.

AI is needed to endow the algorithms with causal reasoning. There is increasing evidence that the warming climate is causing more turbulence, with carbon emissions heating up the atmosphere and increasing wind speeds. When these winds change height, the combination is known as wind shear. According to Professor Paul Williams' research [lix], severe CAT in the North Atlantic has increased by 55 percent since 1979, so emphasis will be put on developing efficient CAT forecasting tools.

Climate is the accumulation of weather and AbsoluteClimo [lx], which does long-term climate prediction planning, can align with the airlines, who plan their routes well in advance, to make use of their modelling for flight-level winds and high-altitude turbulence. A turbulence intensity rating does exist, as shown below courtesy of Weather.Gov [lxi].

Turbulence Intensity Classification	
Intensity	**Effect**
Light	Slight erratic changes in altitude and/or attitude
Moderate	Change in altitude and/or attitude, but the aircraft remains in positive control at all times
Severe	Large, abrupt changes in altitude and/or attitude. Aircraft may be momentarily out of control
Extreme	Aircraft is violently tossed about and practically impossible to control. May cause structural damage.

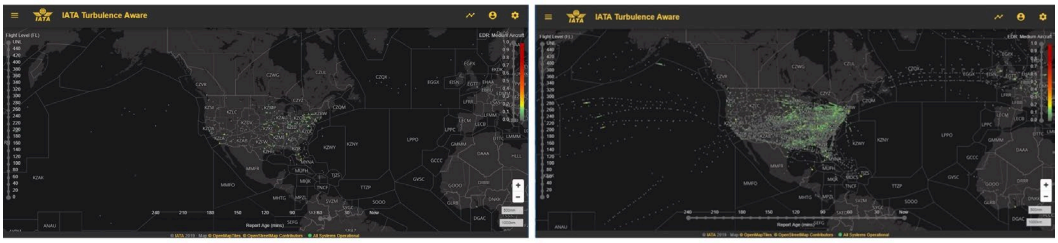
Source: Weather.Gov

These bands can be rated T1-T4 for severity. All catastrophe insurance models are based on severity and frequency. A catastrophe bond around turbulence could be sponsored by an insurer, airline, or even the International Air Transport Association (IATA), with a set of investors such as pension funds and using data models of both stochastic and predictive type.

Event data is difficult to capture as black box information is not pulled unless there is an accident. If we are using T3-T4 as a trigger, data from severe and extreme turbulence is needed and could be used in parametric policies and a secondary trigger could be based on number of

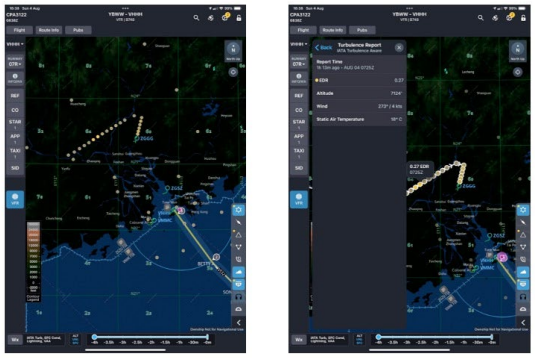
injuries and would pay out straight away. If no event is triggered at the maturity of the bond the investors get a return; and if an event occurs, part or all of their capital would go to paying the claims.

One of the technical innovations is the Turbulence Aware app created by IATA [lxii]. The current products to track and avoid it have significant limitations due to imprecise location, subjectivity, and time lag. Pilots and dispatchers need accurate information pinpointing the location and intensity of turbulence to best advise passengers and crew and optimize fuel burn. Turbulence events can cause an aircraft to divert; but with industrywide sharing of actual occurrences in real time, this could be avoided. The app image below shows the difference of a few airlines reporting turbulence versus multiple airlines.



Source: IATA

The image below shows turbulence tracking and enabling shared reporting by the pilots.



Source: IATA

Airlines are integrating the IATA Turbulence Aware platform with Lido mPilot [lxiii], the Lufthansa mobile navigation solution. This brings shared data to give real-time, highly accurate turbulence information and forecasts, equipping pilots to plot the best paths around affected areas for enhanced safety, efficient navigation, and optimisation of flight plans managing fuel consumption. The member airlines automatically share turbulence reports with all airlines, contributing data to the platform for better situational awareness. A global, industry-wide data exchange platform, Turbulence Aware receives the existing airline data from ground servers, performs quality control, deidentifies data, and provides the data back to airlines via a ground-to-ground, system-to-system connection.

Turbulence is a frequent cause of injuries on airplanes. Every year in the United States, 65,000 aircraft suffer moderate turbulence and 5,500 run into severe turbulence [lxiv], costing $500 million per year from injuries, delays, and damages. In 72 percent of cases there is advance warning, so aircraft can fly around the storm and avoid the turbulence risk. Climate change is modifying turbulence and severe turbulence could double or triple in the coming decades. Southern Cross Travel Insurance has reported a significant rise in turbulence related claims up to 700 percent [lxv]; but it's still a very small percentage of all the travel claim reasons.

Conclusions

Businesses, public services, and computer users across the world faced disruption on July 19, 2024 as a result of the IT outage, which is being named by many as one of the largest and worst cyber events in recent history. Although not a cyberattack or malicious act, it was surprising to many that the outage was caused by such a basic error of patching a computer kernel in production without verifying for misconfigure but this can happen again to any cybersecurity company so improved mitigation should be the outcome to shape here.

The result of the incident was unavailability of systems, but the root cause was a data integrity issue caused by not detecting the fault *a priori*. When software operates in a critical path there should be multiple layers of protection and quality assurance but here something went wrong with the internal test bed. Microsoft stated a 2009 European Union antitrust agreement forced them to sustain low-level kernel access to third-party developers[lxvi]. Also, the Apple Endpoint Security framework [lxvii] can be used instead of a kernel extension and moving away from the kernel approach should be enforced for obvious reasons. The intricacies of this event will play itself out over the next months, but the future implications must be explored in parallel.

All the right things can be done in cybersecurity in terms of measuring and prioritizing; but if the issue is not fixed before an attacker gets to it, then all effort is wasted.

There are seven main key takeaways ensuring the proper mitigation of vulnerabilities against an IT outage but the list is not exhaustive:

1. Knowing the assets in the environment—not only the software/hardware assets, but also the data assets which are often absent. The CMDB must be up to date.

2. Ability to detect vulnerabilities and misconfigurations across all assets in a controlled environment both in the cloud and on premises before moving into production and with the mandate to do the actual fixing/patching.

3. Prioritize by an intelligence perspective what is important from the business angle to focus on fixing high risk vulnerabilities to lessen low risk patching.

4. Collect the data that may contain malware such as browser plug ins and system logs.

5. Integrate risk-based approach strategy with vulnerability management balancing operational and security risk anticipating a constantly evolving threat landscape.

6. Integrate IT and security team efforts leading to automation/orchestration and educate top stakeholders on vulnerability management using a preventative/predictive approach by explaining the root cause of the exposure emphasizing data integrity.

7. Diversify the cybersecurity roducts in policy to reduce aggregation risk.

Companies are on high alert as cyberattacks increase and by 2025 the cost of cybercrime is predicted to grow to $10.5 trillion, according to Cybersecurity Ventures [lxviii]. While the events can result in large financial losses for organizations, there are also reputational damages and security upgrade costs. Cyber risk and recognizing data as an asset have increasingly become a boardroom issue and companies need to put mitigation and risk management measures in place, including the misconfiguration in vulnerability and patch management.

The attack surface is widening and the rise of “ransomware as a service,” where cyber criminals license their tools and know-how to like bad actors and use of AI data poisoning, [lxix] are examples of a changing threat landscape. The aviation sector took the brunt of the outage and faces another peril of increasing turbulence because of climate change where more technology is applied, leading to more technology and endpoint devices to protect.

The outage situation draws parallel to a plane which tragically crashed into the Atlantic Ocean in 1999 and sparked changes in the aviation and insurance sectors on how to improve security on board planes and the mental health of pilots. Nobody thought what would have happened had it been worse. Significantly, a bad actor asked the downward counterfactual question, “If a plane can be plunged into the ocean, it can be crashed into a building”— which was to happen two years later with tragic consequences on 9/11, which changed the world.

Nobody mitigated this downward scenario, which may have altered the outcome if we would have reimagined history from that event in 1999. Now, in 2024, there has been an event in the cyberspace which could have been worse had this been the act of a malicious actor using ransomware and other forms of cyber intrusion. This downward scenario could lead not only to large financial losses but to loss of life through failure of transport technology and healthcare disruptions.

What are the bad actors thinking now? This is a wake-up call to take mitigation action. The difference in 25 years in these events is that we now have the technology in the form of causal AI reasoning that can model these downward counterfactuals at scale and present these outcomes in a predictive manner so that mitigation can be done.

Action must be taken even though it may be perceived July 2024 was a “near miss” and had little impact on the insurance industry. We would expect to see more attention paid to data integrity from the top down in organizations and more to mitigate zero-day exploits, vulnerability management, and endpoint device protection. Silence is not an option.

References

The author would like to acknowledge the work done by Qualys, Guardtime, SyberGRC and other cybersecurity organizations that make these critical mitigation policies possible and adaptable, as well as the research work done by NASA and NCAR in clear air turbulence and IATA for the development of the Turbulence Aware app.

[i] https://connect2amc.com/118-strategic-planning-moltke-the-elder-dwight-eisenhower-winston-churchill-and-just-a-little-mike-tyson#:~:text=The%20German%20field%20marshal%2C%20known,the%20enemy”%20is%20the%20popular

[ii] https://techsafety.org.au/blog/2024/09/02/crowdstrike-the-largest-it-outage-in-history/#:~:text=On%2019%20July%2C%20a%20faulty,affecting%208.5%20million%20Windows%20devices.

[iii] https://en.wikipedia.org/wiki/2024_CrowdStrike_incident

[iv] https://www.spiceworks.com/it-security/endpoint-security/news/crowdstrike-outage-costs-billions-insurance-estimates/#:~:text=Cyber%2Danalysis%20firm%20CyberCube%20has,advised%20caution%20regarding%20cyber%20insurance.

[v] https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

[vi] https://www.techtarget.com/searchwindowsserver/definition/blue-screen-of-death-BSOD#:~:text=The%20term%20blue%20screen%20of,dead%20from%20a%20functional%20perspective.

[vii] https://www.theguardian.com/technology/article/2024/jul/24/crowdstrike-outage-companies-cost

[viii] https://www.reuters.com/technology/microsoft-says-about-85-million-its-devices-affected-by-crowdstrike-related-2024-07-20/

[ix] https://apnews.com/article/singapore-airline-flight-turbulence-c8a890fc3596bc69b766ab9a6e5987bb#:~:text=A%2073%2Dyear%2Dold%20British,an%20emergency%20landing%20in%20Bangkok.

[x] https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.712066/full#:~:text=One%20way%20to%20regulate%20the,studied%20for%20its%20regulatory%20efficacy.

[xi] https://en.wikipedia.org/wiki/Causal_AI

[xii] https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

[xiii] https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/#:~:text=According%20to%20Edgescan%2C%20the%20average,facing%20vulnerabilities%20was%2057.5%20days.

[xiv] https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

[xv] https://www.watchguard.com/wgrd-news/blog/there-was-cyberattack-every-39-seconds-2023

[xvi] https://www.linkedin.com/pulse/how-many-cyber-attacks-happen-per-day-world-prardhana-kennedy-p1wsc#:~:text=Nearly%204000%20new%20cyber%20attacks,malware%20are%20detected%20every%20day.

[xvii] https://www.cobalt.io/blog/cybersecurity-statistics-2024

[xviii] https://www.statista.com/markets/

[xix] https://www.ibm.com/topics/what-is-a-digital-twin

[xx] https://cyvatar.ai/vulnerability-management-system/

[xxi] https://www.cisecurity.org/

[xxii] https://cloud.google.com/security/resources/m-trends

[xxiii] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[xxiv] https://www.cymar.org/

[xxv] https://www.verizon.com/business/resources/articles/machine-state-integrity/

[xxvi] https://www.qualys.com/company/newsroom/news-releases/usa/qualys-expands-enterprise-trurisk-platform-with-cybersecurity-asset/

[xxvii] https://sybergrc.com/

[xxviii] https://www.spiceworks.com/

[xxix] https://www.guycarp.com/company/news-and-events/news/press-releases/business-email-compromise-potentially-overlooked-cyber-threat.html

[xxx] https://www.cashmatters.org/blog/global-cybercrime-losses-exceed-1-trillion

[xxxi] https://en.wikipedia.org/wiki/PowerShell

[xxxii] https://edu.gcfglobal.org/en/internetsafety/installing-and-updating-browser-plugins/1/

[xxxiii] https://guardtime.com/

[xxxiv] https://showroom.demos.guardtime.com/8-mida.html

[xxxv] https://www.nist.gov/

[xxxvi] https://www.jmp.com/en_hk/statistics-knowledge-portal/what-is-correlation/correlation-vs-causation.html#:~:text=Correlation%20tests%20for%20a%20relationship,correlation%20does%20not%20imply%20causation.”

[xxxvii] https://www.researchandmarkets.com/report/causal-ai

[xxxviii] https://vulcain.ai/

[xxxix] https://www.hypr.com/security-encyclopedia/notpetya#:~:text=NotPetya%20takes%20its%20name%20from,but%20the%20resemblance%20ends%20there.

[xl] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[xli] https://www.solarwinds.com/

[xlii] https://www.scribbr.com/methodology/confounding-variables/
[xliii] https://redriver.com/security/target-data-breach
[xliv] https://www.comparitech.com/net-admin/vsoc-virtual-security-operations-center/
[xlv] https://www.ultirisk.com/
[xlvi] https://www.marsh.com/en-gb/services/cyber-risk/expertise/silent-cyber-how-you-can-cover-perils.html
[xlvii] https://insights.cybcube.com/en/crowdout-preliminary-estimate
[xlviii] https://www.wired.com/story/hospitals-crowdstrike-microsoft-it-outage-meltdown/
[xlix] https://blog.talosintelligence.com/threat-source-newsletter-jan-25-2024/
[l] https://www.lenovo.com/us/en/glossary/authenticator-app/?orgRef=https%253A%252F%252Fwww.google.com.hk%252F
[li] https://guardtime.com/platform
[lii] https://www.wptv.com/business/company-news/delta-ceo-says-massive-tech-outage-cost-company-500-million#:~:text=In%20the%20wake%20of%20last,for%20reimbursements%20and%20hotel%20costs.
[liii] https://businesstravelerusa.com/news/delta-faces-loss-crowdstrike-outage/
[liv] https://edition.cnn.com/2024/08/29/us/united-airlines-turbulence-memphis-landing?cid=ios_app
[lv] https://www.flightradar24.com/blog/is-cat-more-common/#:~:text=Clear%20Air%20Turbulence%20(CAT)%20is,is%20not%20usually%20visually%20identifiable.
[lvi] https://oceanservice.noaa.gov/facts/lidar.html#:~:text=Lidar%20—%20Light%20Detection%20and%20Ranging,the%20surface%20of%20the%20Earth.
[lvii] https://science.nasa.gov/mission/cats/#:~:text=CATS%20was%20a%20lidar%20remote,International%20Space%20Station%20(ISS).
[lviii] https://news.ucar.edu/8703/triggering-turbulence-clear-air
[lix] https://research.reading.ac.uk/meteorology-aviation/current-projects/aircraft-turbulence-and-climate-change-dr-paul-williams/
[lx] https://absoluteclimo.com/
[lxi] https://www.weather.gov/source/zhu/ZHU_Training_Page/turbulence_stuff/turbulence/turbulence.htm#:~:text=Severe%20turbulence%20causes%20large%20and,violently%20against%20their%20seat%20belts
[lxii] https://www.iata.org/en/services/data/safety/turbulence-platform/
[lxiii] https://www.lhsystems.com/solutions-services/flight-deck-solutions/lidonavigation/lidompilot
[lxiv] https://time.com/6994422/air-europa-flight-turbulence-injuries-brazil-uruguay-singapore/
[lxv] https://www.insurancebusinessmag.com/au/news/travel/scti-sees-spike-in-turbulencerelated-travel-insurance-claims-494898.aspx#:~:text=Southern%20Cross%20Travel%20Insurance%20(SCTI,related%20claims%20since%20early%202023.
[lxvi] https://www.silicon.co.uk/workspace/operating-system/microsoft-blames-2009-eu-agreement-for-worlds-biggest-it-outage-572752
[lxvii] https://www.sentinelone.com/blog/going-kextless-why-we-all-need-to-transition-away-from-kernel-extensions/#:~:text=Introducing%20Apple's%20New%20Endpoint%20Security,enough%20–%20the%20Endpoint%20Security%20Framework.
[lxviii] https://www.business-standard.com/finance/personal-finance/cybercrime-costs-to-hit-10-5-trn-by-2025-how-insurance-may-save-your-biz-124072400476_1.html
[lxix] https://www.techtarget.com/searchenterpriseai/definition/data-poisoning-AI-poisoning

9.2024

David Piesse
CRO of Cymar

About the Author:
David Piesse is CRO of Cymar. David has held numerous positions in a 40-year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.