Harmonizing Cyber Risk Management

INTEGRATING GOVERNANCE AND TECHNICAL CONTROLS FOR EFFECTIVE INCIDENT MITIGATION AND RESILIENCE

Contents

EXECUTIVE SUMMARY

As cyber-attacks become increasingly common and sophisticated, organizations must prioritize incident response planning to minimize damage and prevent further compromise. Effective incident response requires a combination of technological tools, intelligent systems, and well-defined procedures alongside the different Governance Risk & Compliance (GRC) control standards in each industry.

But how can Board Members, C-Suite, and Stakeholders agree on a budget for cyber risk investments when the needs of the organization are many? Which risks are the most critical for the organization to choose when Technical controls are in competition with GRC control requirements? How best to align them for cost-efficiency? Historically, many cyber disasters are the result of organizations being unable to distinguish between existence-threatening incidents and minor incidents, especially when they have more than one urgent cyber risk in mind.

Comparatively, highly experienced emergency physicians must make similar prioritizations. They reveal that the reasons for their "cool state of mind" are the routines and practices that quickly identify which injuries are life-threatening and which are minor. If "life or death" is the metric at ER, what is the metric for cyber-related risks?[1]

This white paper provides an in-depth exploration of how to effectively link an organization's Technical Controls with its Governance Controls in a manner that clearly identifies the highest-priority risks. This approach can reduce misunderstandings and enable C-Suite executives to fulfill cost-effective Cyber Risk Management, and Stakeholders to prioritize the incident response aligned with organizational objectives.

[1] Çavuş, D. M. (n.d.). (tech.). From Qualitative Analysis to Quantitative Risk Analysis. London: MonteCarloPlus.com.

INTRODUCTION

The prevailing landscape of cyber threats is characterized by its sophistication, frequency, scope, and impact. Concurrently, this phenomenon intersects with a scarcity of Information Technology (IT), or Information Security (InfoSec) professionals adept at navigating the compound technological complexities of this perpetually evolving digital landscape. An Incident Response Plan, also called a Security Incident Response Playbook (see Appendix A) is a set of living documents centered around detecting, analyzing, responding, and resolving cybersecurity incidents. In short, they are procedural controls used by InfoSec.

Governance Controls, however, encompass a broader set of policies, standards, procedures, and guidelines that define the overall framework for managing and directing InfoSec.

This white paper will elaborate on the relationship between a Security Incident Response Playbook, the current industry standard Best Practices (Appendix B) for incident response, and how to tether these Procedural Controls to the Governance Risk and Compliance (Appendix C) objectives of any organization, using correlations between incident severity and GRC objectives.

BACKGROUND AND CONTEXT

Procedural Controls: Security Incident Playbooks and Best Practices Objectives

As mentioned above, Security Incident Response Playbooks typically provide detailed guidance, methodologies, and frameworks for effectively handling and responding to security incidents. They outline step-by-step technical procedures and recommended actions to detect, contain, mitigate, and recover from security incidents. These "books" serve as valuable references and practical resources for incident response teams to follow when addressing security incidents.

Best Practices are a set of recommended guidelines, strategies, and methods that should be followed to protect digital assets. These practices are developed based on industry experience and the evolving threat landscapes. Best practices consolidate the collective knowledge and expertise of cybersecurity professionals.

In terms of hierarchy, Best Practices are informed by the content found in Security Incident Response Playbooks, using metrics like MTTD (Mean Time To Detection) and MTTR (Mean Time To Resolution) as part of the Key Performance Indicators (KPI) that determine the success of these Best Practices and the Security Incident Response Playbook practices. Together, these inform the IT Security controls and standards of an organization, which are enforced by an IT Security team.

Governance Controls: Governance Risk and Compliance Objectives

Governance controls encompass a broader set of policies, standards, procedures, and guidelines that define the overall framework for managing and overseeing IT Security. Governance controls involve organizational strategy, objectives, approach and tactics, and risk management with both quantitative and qualitative definitions. Furthermore, governance controls enforce compliance with governance policies and regulatory obligations; they may also include adherence to standards such as NIST, ISO, and GDPR.

Governance Controls extend from Global to Regional to Local to Industry-specific standards. For example, a boutique hotel group may to comply with the General Data Protection Regulation (GDPR) concerning its European guests, the California Consumer Privacy Act (CCPA) for guests located in California, and the Payment Card Industry Data Security Standard (PCI-DSS).

All policies and standards relevant to these best practices and regulations are established and enforced by the Board of Directors, executive and senior management, internal and external auditors, and specific practitioners like IT Personnel, Compliance Analysts, and Risk Managers.

In many (if not most) organizations, there is a severe disconnect

Having presented the imperatives at the IT security operational level (security Incident Response Playbooks and industry best practices) and the corporate governance level (Governance Risk and Compliance), the efficient and effective melding of these two levels is required.

Netswitch Compliance Tethering

Netswitch has developed a cyclical process that we've dubbed *Compliance Tethering,* which integrates IT Security operational imperatives with corporate compliance requirements. With this automation, and through the analysis of both, an organization can:

1. Assess how quickly the organization can detect an attack and threats (decreasing the MTTD).
2. Reduce the false positives with Artificial Intelligence solutions.
3. Align the severity of incidents with governance objectives for response prioritization, based on defining Service Level Agreement (SLA) and Service Level Objectives (SLO) (decreasing the MTTR).
4. Capture Service Level Indicators (SLI) based on defined objectives and risk trending analysis and reform SLO.
5. Quantify the SLI and risk trends into visualized data to begin the Cyber Risk Management journey (*see Unity and Risk Prism below*).

PROBLEM STATEMENT

Problem: Governance Risk and Compliance Objectives and Netswitch

As mentioned above, recent cybersecurity objectives have evolved to include Governance, Risk and Compliance (GRC) objectives to streamline processes of risk and control. Often the GRC objectives require IT & Cybersecurity technical data and control processes to support company objectives.

Most companies' Best Practice policies (as regards technical controls such as access controls, firewalls, encryption and IDS/IPS etc.), must align with their GRC controls (policy and procedure, risk management, compliance, data management etc.). For example, within the pharmaceutical industry, the organization must comply with HIPAA and the NIST CSF or ISO27001.

However, within these regulatory structures, there are many controls, sub-controls, and safeguards which require compliance, and it is often difficult for an organization or the Security Operation Center to

prioritize using the general interpretation of Common Vulnerability Scoring System (CVSS). The CVSS, as its term suggested, is often too 'common' to give helpful direction and is often ineffective when tethering the Governance Controls.

This issue stems from the necessity to conform to numerous regulatory frameworks, resulting in a lack of prioritization. This frequently gives rise to what Netswitch refers to as "Acronym Battle," a scenario wherein various departments compete to prioritize their respective controls and processes. As has been historically observed, when two groups are lack effective communication, gaps will occur; and, in this case, those gaps likely lead to cyber risk and data breaches, (see 2017 Equifax Breach) where hackers exploited the unpatched vulnerability, gaining unauthorized access to Equifax's systems and compromising sensitive information of approximately 143 million consumers.

It is important to note, as with this breach, that there can be significant reputational loss, regulatory penalties, and monetary loss from data breaches. In addition to the compromise of sensitive information, Equifax was also fined $700m for this breach, and their shares dropped 13.2 points the first weekend following[2] (See APPENDIX D).

Problems and risks like these lead to a "Vicious Cycle of Self-Destruction" wherein Business Executives become frustrated with spending into a blackhole of cybersecurity tools, and Governance and Technology practitioners become burnt-out because their objectives, expectations, and measurements are not well aligned (See APPENDIX E).

PROPOSED SOLUTIONS

Solution: Governance Risk and Compliance Tethering with Netswitch

In the previous sections we have outlined the statistics and consequences of data breaches, some of which include regulatory fines, economic harm, and reputational loss. It is safe to say, most companies understand the correlation between these consequences and data breach; however, it can be hard to understand the real-time hazard correlations between threats and vulnerabilities and which controls to prioritize for the safeguarding of the company.

If we can solve that problem and assist companies' correlation of their threats to GRC Objectives, the result would be increased collaboration, greater cost efficiency, and enhanced operational efficacy.

---

[2] Shell, A. (2017, September 18). "Equifax image is battered by data breach as consumers feel violated." USA Today. https://www.usatoday.com/story/money/2017/09/18/equifax-image-battered-data-breach-consumers-feel-violated/677908001/

But how exactly do we make these priorities clear?

Within an emergency room, there are highly experienced healthcare professionals who can assess the situation on a large scale, determining the level of urgency between each patient, and in some cases, triage based on severity and life-threatening conditions. In Cybersecurity, we must use similar triage methodology to combine People, Technology and Process, using Augmented Intelligence to prioritize and minimize the volume of incidents organizations have to manage.

Enter Netswitch's CyberRisk Governance™ System

Netswitch's CyberRisk Governance™ (CRG®) System helps solve the "Acronyms Battles" by accelerating cyber resilience defined by governance and Cyber Risk mitigation. It progresses step-by-step to balance limited resources with the technical and GRC control tactics, and it provides augmentation to fill resource gaps, as well as automation to increase cyber resilience.

Likewise, it utilizes an interface called *Unity Risk Indicator*® to provide the visual data needed to identify the prioritized controls allowing stakeholders to communicate priorities based on the company's objectives, budget, and internal resources.

Unity Risk Indicator is:

- *A Single Pane of Glass*: that allows visual and contextual correlations
- *Vendor Neutral*: Facilitating seamless integration with diverse technology solutions, including Open-Source alternatives.
- *Data Driven*: Leveraging transparent data visualization, aggregation, correlation, and preemptive intelligence techniques.
- *Compliance Tethering*: Establishing a connection between data analysis and task-level alignment within the realms of Technical, Governance, Risk, and Compliance (GRC) Controls.
- *Hyperautomation*: Employing autonomous processes to maintain impartiality and cost-effectiveness while enhancing data privacy and sovereignty.

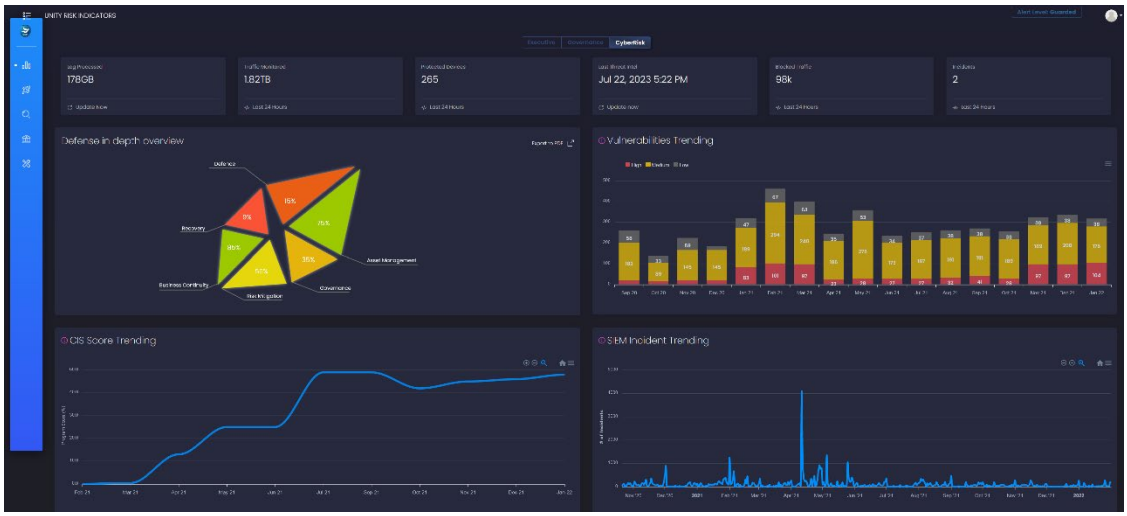

Figure 1: Single Pane of Glass Data Visualization as per Netswitch Unity Risk Indicator

If you are uncertain about starting your company's journey toward enhancing its cyber resilience, an effective starting point lies in conducting a security and risk assessment, Netswitch refers to this as SARA Baseline. This assessment is characterized by full automation, ensuring unbiased results. It entails a comprehensive gap analysis, employing industry benchmarks to identify prioritized vulnerabilities. Additionally, it simulates potential remediation strategies, thereby establishing a solid foundation for the subsequent stages of the improvement process.

RiskPrism®

As an organization matures through its application of Netswitch CRG and its reliance on Unity and the Unity Risk Indicator, it is possible to hasten the incident response by leveraging an additional avenue for enhanced Compliance Tethering communications. Netswitch has integrated a licensed technology – the RiskPrism Decision Support System – to *further* enhance Compliance Tethering. RiskPrism is composed of two components:

RiskPrism Maturity

RiskPrism maturity simplifies and localizes the industry-standard Capability Maturity Model (CMM) assessment of an organization against the NIST Cybersecurity Framework (NIST CSF); Deloitte, KPMG, EY, PwC, and many smaller companies such as Clearwater and Protiviti offer this assessment to enhance risk oversight, but RiskPrism Maturity provides the same results without exorbitant assessment fees.

RiskPrism Maturity differs from the yearly "snapshots" of maturity assessment consultants by:

- Providing an organization-specific application that allows personnel assignment and task management that is performed *throughout the year*.

- Presenting the NIST CSF items – functions, categories, and subcategories – in an easily consumable hierarchical view.
- Allowing for assignments of NIST CSF items to multiple personnel for divergence testing and crowdsourced responses.
- Captures the proximity of the assessor to the NIST CSF item; the closer an assessor is to the NIST CSF item, the more likely it is that the response will be accurate.
- Extends the hierarchical "tree" for each item to track specific risk controls.

RiskPrism Analytics

RiskPrism Analytics is a proprietary and patented technology (USPTO 10,686,825) that considers available elements of risk that are or should be monitored within an organization. RiskPrism facilitates the distributed identification of assets and their associated potential impact values and calculates event probabilities from a comprehensive and expandable set of sources:

- The organization's *RiskPrism* Maturity assessment information.
- Hardware, operating system, application, data, and all associated potential impact values from existing resources.
- Extant vulnerabilities and configuration weaknesses that are present in the IT environment, coupled with data from the National Vulnerability Database.
- Underlying event data maintained by IT Security devices. This is especially important, as IT personnel shortages and the advent of SIEMS has led to "tuning out" low-priority events in favor of events that *appear* significant, leaving the low-priority events and historical analysis to periodic reporting.
- Ancillary company data sets such as personnel and training databases, which can, for example, gauge an employee's sentiment toward the company and/or his performance on IT Security training.
- Intelligence sources such as proprietary sources and the Open Threat Exchange.
- Any *other* data source that can provide risk element data information.

Once RiskPrism acquires and aggregates the two requisite risk elements for risk calculation – probability and potential impact – it calculates the range of absolute risk for each asset using Monte Carlo simulations, determines the most likely value for aggregated risk, and presents the risk results in a format optimized for various consumers of the risk calculations throughout the organization; C-Level personnel can receive a risk value in dollars and *IT personnel can receive a prioritized ordinal list of risks that they can address in real time*. Because of its quantitative nature, RiskPrism also facilitates other financial calculations such as VaR –critical to the financial services and insurance industries – and return on investment (ROI) of security efforts.

CONCLUSIONS

As has been outlined in the previous sections, there are many components to helping companies understand the risk and threats of the cyber industry, and while measuring the KPI's of Best Practices may be the most effective way at protecting a company from cyber threats, we've also detailed how challenging it can be to prioritize the most threatening risks, because of the competing values of our IT Security and Governance Controls.

To highlight once more, one of the key competitive differentiators within Netswitch, CRG (CyberRisk Governance) System is its Compliance Tethering. Instead of pivoting from purely a technical standpoint, or prioritizing only GRC controls, Netswitch will allow for tethering of both to help the C-Suite and Board prioritize and communicate these priorities.

In this way the organization can use their GRC as the objectives that prioritize their technical incidents, thus saving the company reputational and monetary loss resulting from breaches and fines.

About Netswitch, Inc.:

Since 2000, Netswitch, Inc. has been a trusted name in cybersecurity, serving a diverse client base of small and mid-size businesses. We are a leading provider of comprehensive cyber risk solutions.

Guiding Cybersecurity Excellence

Netswitch is a dedicated partner in guiding organizations through the complexities of cyber risks.

Practical Solutions for Resilience

We understand that navigating the cybersecurity landscape can be challenging. Many clients begin their journey with us due to the overwhelming nature of the cyber risks. We provide actionable insights and effective processes to empower organizations.

Holistic Risk Management

Our approach extends beyond technology. We conduct logical security assessments to evaluate overall security posture, aligning solutions with organizational objectives, with available resources and regulatory requirements.

Recognized Innovation

Acknowledged as a "Pioneer" by Gartner® in Managed Detection and Response (MDR) Cybersecurity, Netswitch continues to innovate. Our patented CyberRisk Governance™ system, ensures comprehensive cyber risk understanding and alignment with compliance frameworks.

Contact Us:

For more information about Netswitch, Inc. and how we can assist your organization in achieving Cyber Risk reductions, please reach out to us at www.netswitch.net, info@netswitch.net, or LinkedIn.

Acknowledgments:

We would like to express our gratitude to Mustafa Çavuş PhDv, and Frederick Doyle, CISSP, CRISC, PMC-III for their valuable insights and contributions to this white paper.

APPENDIX A: Security Incident and Response Playbook

A Security Incident Response Playbook should encompass essential elements designed to guide an organization's response to security incidents. These elements collectively contribute to a well-structured and organized approach to managing security incidents, enabling organizations to respond swiftly, decisively, and effectively to mitigate potential damage and minimize disruption. Key elements of a Security Incident and Response Playbook typically include:

1. **Incident Classification**: Clearly defined criteria for categorizing incidents based on severity, impact, and urgency to facilitate appropriate prioritization and resource allocation.
2. **Roles and Responsibilities**: Designation of specific roles and responsibilities for incident response team members, outlining their duties, decision-making authority, and communication protocols.
3. **Incident Detection and Reporting**: Procedures for detecting and identifying security incidents, including the use of monitoring tools, intrusion detection systems, log analysis, and user reports.
4. **Communication and Notification**: Guidelines for notifying relevant stakeholders, both internal and external, including legal teams, executive leadership, affected departments, customers, partners, and regulatory authorities.
5. **Escalation Procedures**: Clearly defined steps for escalating incidents to higher management levels, particularly in the case of critical or widespread incidents requiring immediate attention.
6. **Containment and Eradication**: A step-by-step process for containing the incident, preventing its spread, and eradicating the threat from affected systems.
7. **Evidence Handling and Preservation**: Protocols for collecting, preserving, and documenting evidence related to the incident, ensuring it remains admissible for legal or regulatory purposes.
8. **Analysis and Investigation**: Procedures for analyzing the incident, determining its root cause, and identifying affected systems, data, or assets.
9. **Recovery and Remediation**: Strategies for restoring affected systems and services to their normal functioning state, as well as implementing remediation measures to prevent future incidents.

10. **Post-Incident Review**: Guidelines for conducting a thorough post-incident review and analysis to identify lessons learned, areas for improvement, and opportunities to enhance incident response procedures.
11. **Legal and Regulatory Compliance**: Consideration of legal and regulatory obligations that must be met during incident response, such as data breach notification requirements.
12. **Documentation and Reporting**: Requirements for documenting all actions taken, decisions made, and communications throughout the incident response process, culminating in comprehensive incident reports.
13. **Training and Exercises**: Plans for ongoing training and simulations to ensure incident response team members are well-prepared and capable of effectively responding to various scenarios.
14. **Coordination with External Partners**: Protocols for collaborating with external partners, such as law enforcement agencies, cybersecurity experts, third-party vendors, and public relations teams.
15. **Continuous Improvement**: Mechanisms for continuously updating and refining the playbook based on lessons learned from incidents, changes in the threat landscape, and evolving organizational needs.

APPENDIX B: Best Practices for Incident Response and Supplementary Netswitch Solutions

The current industry standard of Best Practices for Incident Response are as follows:

1. **Quick Detection**: Quick detection of an attack is crucial in minimizing damage and preventing further compromise. Organizations can achieve quick detection through various means, such as intrusion detection and monitoring tools, log analysis, and user behavior analytics. By using these tools, organizations can identify attacks in real-time and prevent further damage.
    - *Netswitch's SIEM Solution— Security Information and Event Management software—allows Continuous Detection with Automation enabling organizations to detect faster and more consistently than ever before.*
2. **Elimination of False Positives**: False positives can be a significant burden on incident response teams, as they can waste valuable time and resources. Implementing intelligent systems that can accurately differentiate between real threats and false alarms can help streamline the incident response process and reduce false positives.
    - *It is an industry concern that the false positives have grown too numerous for the "Human" workforce to handle. Therefore, Netswitch's SIEM Solution utilizes AI and Behavioral Analytics to reduce false positives.*
3. **Identification the Pivot of an Attacker**: Identifying the pivot of an attacker refers to the ability to track their movements and identify the various points in the network they have accessed. This can help incident response teams determine the scope of the attack and identify any vulnerabilities that the attacker may be exploiting. Organizations can use techniques such as network forensics and malware analysis to identify the pivot of an attacker.
4. **Rapid Communication and Notification**: Rapid communication and notification of the incident response team is essential to minimize damage and prevent further compromise. Service Level Agreements (SLAs) can help ensure that teams are notified promptly and given the resources

they need to respond effectively. Organizations should establish clear lines of communication and escalation procedures to ensure that incidents are addressed promptly and effectively.
    - *Netswitch utilizes the interface called Unity Risk Indicator, which allows for a 'single pane of glass' display for Stakeholders, Business Executives, Governors and Technologists. Through this platform, they will be able to view objectives, then Service Level Agreements (SLA) Service Level Objectives (SLO) and finally Service Level Indicators (SLI).*
5. **Clear Definitions, Roles and Workflows**: A well-defined incident response playbook can help teams respond quickly and efficiently to an attack. This should include procedures for detection, analysis, containment, eradication, and recovery. Regularly testing and updating the playbook can help ensure that teams are prepared to respond effectively to new and evolving threats. Organizations should also establish roles and responsibilities for incident response team members and provide training to ensure that they are equipped to respond effectively.
    - *There are many ways in which the Security Incident Response Playbooks need modification and complementing to keep up with the changing and evolving threat landscape, as will be reviewed in length below. Netswitch employs the use of ABCD technologies to shore up any organizations' incident response.*

By prioritizing and implementing these Best Practices along with the augmentation of Netswitch's systems, organizations can better protect themselves against cyber-attacks and minimize damage when incidents occur.

APPENDIX C: Governance, Risk and Compliance

Governance controls encompass a wide range of policies, procedures, and guidelines that establish the framework for IT security management. They encompass strategic decision-making, risk management, and adherence to legal and regulatory standards like NIST Framework, ISO, and COBIT. Typically overseen by senior management, executive boards, or regulatory bodies.

Security Incident Response Playbooks and Best Practices can align with an organization's Governance Risk and Compliance (GRC) objectives through Compliance Tethering. GRC objectives establish the strategic framework for incident response, ensuring alignment with goals like data protection, compliance, and stakeholder trust.

Examples of governance controls include:

1. **Policies and Procedures**: Governance controls encompass the development and implementation of policies and procedures that define the organization's governance principles, ethical standards, and expected behaviors. These policies may cover areas such as conflicts of interest, code of conduct, whistleblower protection, and board governance.
2. **Risk Management**: Effective governance controls involve integrating risk management processes into decision-making. This includes identifying and assessing risks, establishing risk appetite and tolerance levels, and implementing risk mitigation strategies. Governance controls may also involve regular reporting and monitoring of key risks to the board and senior management.
3. **Controls**: Governance controls include establishing internal controls to ensure the accuracy, reliability, and integrity of financial reporting and asset safeguarding. Internal controls may cover

areas such as segregation of duties, access controls, authorization processes, and monitoring of key controls.

4. **Compliance Management**: Governance controls encompass the establishment of a compliance management framework to ensure adherence to relevant laws, regulations, and internal policies. This includes conducting regular compliance assessments, implementing compliance monitoring, and reporting mechanisms, and providing training and awareness programs to employees.
5. **Performance Management**: Governance controls involve the establishment of performance management systems that link strategic objectives to key performance indicators (KPIs) and targets. This enables monitoring and evaluation of performance against established goals and ensures alignment with the organization's strategic direction.
6. **Transparency and Reporting**: Governance controls emphasize the need for transparent and timely reporting of relevant information to stakeholders. This includes financial reporting, disclosure of material information, and regular communication of governance-related matters to shareholders, employees, regulators, and other relevant parties.
7. **External Audit and Assurance**: Governance controls often involve engaging external auditors or independent third parties to provide assurance on the organization's financial statements, internal controls, and compliance with applicable regulations.

In summary, Governance controls establish the overarching structure and framework for IT security, including the establishment of policies, procedures, and risk management strategies. They ensure that the organization's security objectives align with business goals and comply with relevant regulations and standards.

APPENDIX D: Equifax Data Breach (2017)

Equifax is one of the largest credit reporting agencies in the United States. Like most agencies it too operates under GRC controls (policies, procedures, and regulatory compliance requirements) to ensure data security and privacy. Also, they have many technological controls and safeguards implemented to protect sensitive data from unauthorized access.

However, in 2017 there was a massive data breach attributed to a vulnerability in the Apache Strus web application framework, which Equifax failed to patch in a timely manner. In this case, the vulnerability had been recognized, and a patch had been released months before the breach. But the failure to apply the patch and update the vulnerable software in a timely manner led to the breach.

In hindsight, it is reasonable to postulate that the IT team responsible for managing and updating the company's software systems may have prioritized other technical tasks or projects. They may have also been under pressure to complete other projects or might not have recognized the urgency of the patch due to a lack of communication and coordination with the Governance, Risk and Compliance team.

Likewise, the GRC team that held the responsibility of ensuring compliance with the regulatory requirements, monitoring and assessing risk and establishing policies, may not have communicated the urgency of the vulnerability, or did not emphasize the importance of the patch.

In any scenario, the competing priorities between GRC controls and technical controls, along with the lack of systems to prioritize and communicate that priority, resulted in a failure to address the known

vulnerability in a timely manner. As a result, hackers exploited the unpatched vulnerability, gaining unauthorized access to Equifax's systems and compromising sensitive information of approximately 143 million consumers.

This incident highlights the importance of effective coordination and collaboration between GRC and technical teams. Failure to align these priorities and bridge the gap between GRC and technical controls can lead to critical oversights, leaving vulnerabilities unaddressed and exposing organizations to significant risks.[3]

APPENDIX E: Statistics on Data, Reputational and Financial Loss as a Result of Fines and Breaches

Statistical Financial Loss as a Result of Breach

Data breaches can have significant financial consequences for companies and organizations. While specific statistics may vary depending on the industry, the size of the company, and the nature of the breach, several studies and reports provide insights into the fiscal impact of data breaches.

[3] Shell, A. (2017, September 18). "Equifax Image Is Battered by Data Breach as Consumers Feel Violated." USA Today. https://www.usatoday.com/story/money/2017/09/18/equifax-image-battered-data-breach-consumers-feel-violated/677908001/

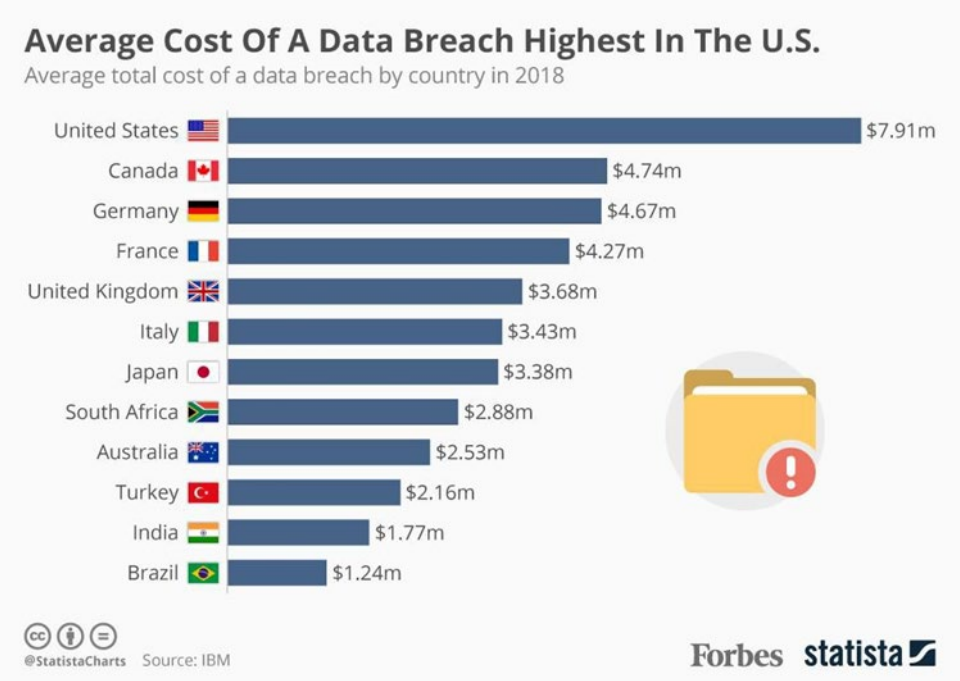

Figure E1: Average Cost of a Data Breach by Country, 2018[4]

Statistical Regulation Penalties as a Result of Breach

Quantifying the exact regulatory penalties resulting from data breaches can vary significantly depending on the jurisdiction, applicable laws, and the specific circumstances of each breach. However, several high-profile cases provide insights into the potential financial impact of regulatory penalties imposed on companies following data breaches. Some districts have implemented or are considering even more stringent data protection regulations, which could potentially result in higher penalties for data breaches in the future.

[4] Martin Gontovnikas Former SVP of Marketing and Growth (2018, October 5). "What is a data breach?". Auth0. https://auth0.com/blog/what-is-a-data-breach/

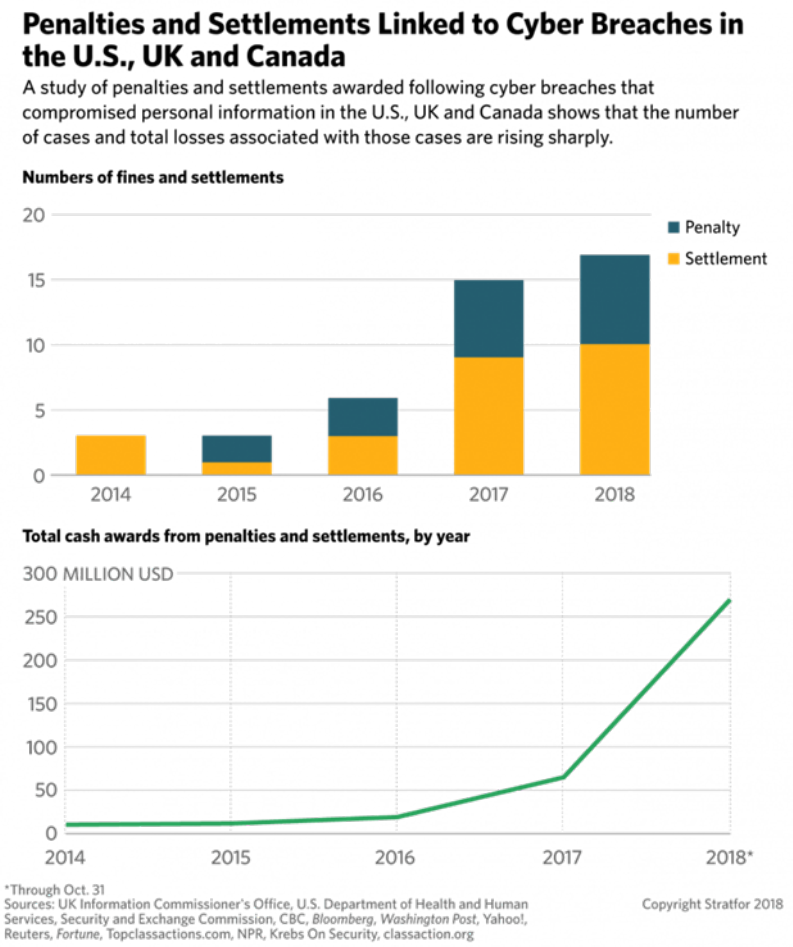

Figure E2: Graphic example of how Data Breaches Impact Company Reputation[5]

Statistical Reputational Loss as a Result of a Breach

Quantifying the exact reputational loss caused by data breaches is challenging, as it can vary depending on numerous factors such as the company's brand image, the severity of the breach, the effectiveness of the response, and public perception. However, studies and reports have shown that data breaches can have a significant negative impact on a company's reputation.

[5] "Fines And Lawsuits Are Adding To The Cost of Corporate Data Breaches." Stratfor. (2018, November 13). https://worldview.stratfor.com/article/fines-and-lawsuits-are-adding-cost-corporate-data-breaches

Figure E3: Graphic example of how Data Breaches Impact Company Reputation[6]

These statistics highlight the significant impact that data breaches can have on a company's reputation. Rebuilding trust and repairing damaged reputation can be a long and challenging process, requiring transparent communication, swift and effective response, and proactive measures to prevent future breaches.

Figure E4: Graphic example of consumer perception of Target Brand before and after breach[7]

[6] Buckbee, M. (2022, February 25). "Analyzing Company Reputation After A Data Breach." Varonis. https://www.varonis.com/blog/company-reputation-after-a-data-breach

[7, 8] Buckbee, M. (2022, February 25). "Analyzing Company Reputation After A Data Breach." Varonis. https://www.varonis.com/blog/company-reputation-after-a-data-breach

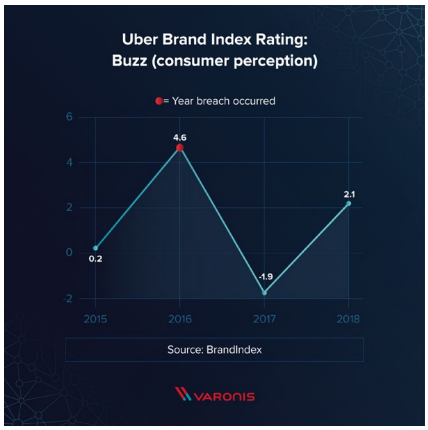

Figure E3: Graphic example of consumer perception of Uber Brance before and after breach[8]

REFERENCES

1) Buckbee, M. (2022, February 25). Analyzing company reputation after a data breach. Varonis. https://www.varonis.com/blog/company-reputation-after-a-data-breach
2) Çavuş, D. M. (n.d.). (tech.). From Qualitative Analysis to Quantitative Risk Analysis. London: MonteCarloPlus.com.
3) ChatGPT, personal communication, July, 2023
4) Stratfor (2018, November 13). "Fines And Lawsuits Are Adding to The Cost of Corporate Data Breaches". https://worldview.stratfor.com/article/fines-and-lawsuits-are-adding-cost-corporate-data-breaches
5) Martin Gontovnikas, Former SVP of Marketing and Growth at Auth0, (2018, October 5). "What is a data breach?" Auth0. https://auth0.com/blog/what-is-a-data-breach/
6) Risk.net staff, Mar 2023, et al. "Top 10 Operational Risks for 2023." Risk.Net, 20 June 2023, www.risk.net/risk-management/7956128/top-10-operational-risks-for-2023

Shell, A. (2017, September 18). “Equifax Image Is Battered by Data Breach as Consumers Feel Violated”. USA Today. https://www.usatoday.com/story/money/2017/09/18/equifax-image-battered-data-breach-consumers-feel-violated/677908001/