Top Threats to Cloud Computing: Deep Dive

A case study analysis for 'The Treacherous 12: Top Threats to Cloud Computing' and a relative security industry breach analysis

cloud security alliance®

Forward

CASE STUDY PROJECT GENESIS

In 2012, Cloud Security Alliance (CSA) produced a survey that helped articulate cloud computing's most significant and pressing issues. At the time, the cloud was a relatively new concept, and this content filled a significant gap by providing valuable industry insight.

The CSA derived the original "Top Threats" (TTs) title from the first survey and became the foundation of this case study. However, security professionals recognize that the "Notorious Nine" and "Treacherous Twelve" threats provide only a fraction of the whole picture. Other factors for consideration include actors, risks, vulnerabilities and impacts.

To address these missing elements, the Cloud Security Alliance Top Threats Working Group decided the next document released should address more technical details dealing with architecture, compliance, risk and mitigations.

Hence, the creation of this document.

This case study collection addresses the limitations of the anecdotes and case studies identified within the TT documents by providing additional details and actionable information. Ideally, these data identify where and how TTs fit in a greater security analysis, while providing a clear understanding of how lessons and concepts can be applied in real-world scenarios.

THE TOP THREATS WORKING GROUP RECENT CONTRIBUTIONS

The "2017 Top Threats" document cites multiple recent examples of issues found in the "Treacherous Twelve" survey results. While these anecdotes allow cybersecurity managers to better communicate with executives and peers (and provide context for discussions with technical staff), they do not provide in-depth detail of how everything fits together from a security analysis standpoint.

WHAT YOU WILL FIND

This case study attempts to connect all the dots when it comes to security analysis by using nine anecdotes cited in the TTs for its foundation. Each of the nine examples are presented in the form of (1) a reference chart and (2) a detailed narrative. The reference chart's format provides an attack-style synopsis of the actor, spanning from threats and vulnerabilities to end controls and mitigations. We encourage architects and engineers to use this information as a starting point for their own analysis and comparisons.

The longer-form narratives provide additional context (such as how an incident came to pass or how it should be dealt with). For cases where details—such as impacts or mitigations—were not discussed publicly, we extrapolated to include expected outcomes and possibilities.

We hope you see this effort as useful and welcome any feedback and/or participation for upcoming publications.

To your future success,

Jon-Michael C. Brook, CISSP, CCSK
Co-chair, Top Threats Working Group

Table of Contents

Acknowledgments

Many thanks to the team that made this happen; this much work would not succeed without their involvement.

CO-CHAIRS

Jon-Michael C. Brook, CISSP, CCSK
Scott Field
Dave Shackleford

CONTRIBUTORS

Randall Brooks
Alex Getzin
Aiyan Ma
Michael Roza
Shira Shamban
Velan Thangavelu
Mark Yanalitis

CSA RESEARCH

Victor Chin
Shamun Mahmud

‘Top Threat’ Coverage by Case Study

TOP THREATS ITEM #	LINKEDIN	MONGODB	DIRTY COW	ZYNGA	NET TRAVELER	YAHOO!	ZEPTO	DYNDNS	CLOUDBLEED
TT 1									
TT 2									
TT 3									
TT 4									
TT 5									
TT 6									
TT 7									
TT 8									
TT 9									
TT 10									
TT 11									
TT 12									

The case studies selected represent each of the 12 “Top Threats.”

Recommended Cloud Controls Matrix (CCM) Domains for Case Study:

CCM CONTROL DOMAIN	LINKEDIN	MONGODB	DIRTY COW	ZYNGA	NET TRAVELER	YAHOO!	ZEPTO	DYNDNS	CLOUDBLEED
AIS			X	X					
AAC			X		X			X	
BCR			X		X		X	X	
CCC			X						X
DSI				X					
DCS									
EKM	X								X
GRM	X		X			X		X	
HRS		X	X	X	X	X	X		
IAM	X	X	X	X			X		X
IVS	X							X	X
IPY									
MOS									
SEF	X			X	X	X	X	X	
STA									
TVM	X	X			X	X	X	X	X

ANALYSIS

Mitigations and controls applicable to the nine case studies cover 13 of the 16 Cloud Controls Matrix (CCM) domains. Data Center Services (DCS) and interoperability and portability (IPY) controls principally cover data center operations at cloud service provider facilities, not matching the case studies or “Top Threats” identified for cloud computing. Mobile security (MOS) controls are used in relation to mobile endpoint protection, and include safeguards typically utilized in enterprise environments. Supply Chain Management, Transparency and Accountability (STA) controls are also not represented.

Case Study CCM Control Coverage

CCM CONTROL DOMAIN	LINKEDIN	MONGODB	DIRTY COW	ZYNGA	NET TRAVELER	YAHOO!	ZEPTO	DYNDNS	CLOUDBLEED
TVM	X	X			X	X	X	X	X
HRS		X	X	X	X	X	X		
SEF	X			X	X	X	X	X	
IAM	X	X	X	X			X		X
GRM	X		X			X		X	
BCR			X		X		X	X	
AAC			X		X			X	
IVS	X							X	X
AIS			X	X					
CCC			X						X
EKM	X								X
DSI				X					
IPY									
MOS									
DCS									
STA									

The domains in the chart above are sorted according to how often controls in those domains are relevant as a mitigating control.

Threat and Vulnerability Management (TVM), in particular Vulnerability/ Patch Management (TVM-02), would have been useful in detecting many of the vulnerabilities that were exploited in these incidents.

Human Resources Security (HRS)—and specifically security training—were identified as possible mitigations in six of the nine case studies, as was Security Incident Management, E-Discovery and Cloud Forensics (SEF). Based on these results, one can conclude that planning for an attack fallout and executing on that plan was paramount to successfully dealing with two-thirds of the incidents cited. Furthermore, Identity and Access Management (IAM) controls were determined to be relevant mitigation for more than half of the incidents.

LinkedIn (Password Hack 2012)

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
Internal Skipped basic standards	**TT 11** Denial of Service	**TT 2** Insufficient Identity, Credential and Access Management	**TT 1** Data Breach Loss of user credentials, PII.	**Financial** – Forensics and cleanup cost $1M – Users lawsuit $1.25M (not including legal fees	**Preventative** – EKM-02 – IAM-12 – GRM-03 – GRM-06
				Operational – TWO calls to users to reset their passwords	**Detective** – IVS-01 – IVS-06 – SEF-04 – GRM-05 – GRM-10 – TVM-02
External Malicious hacker—Eastern European	**TT 12** Shared Technology Vulnerabilities		**TT 5** Account Hijacking, using the stolen passwords (password re-use in other services)	**Compliance** – Failure to protect PII	**Corrective** – GRM-07 – GRM-08 – GRM-09 – SEF-01 – SEF-05
				Reputational – Negative impacts on long term service usage	

ATTACK DETAILS

Threat actor: Russian citizen Yevgeny Nikulin was arrested by Czech police for his alleged involvement in the LinkedIn breach.

Threat: The hacker stole a LinkedIn employee's credentials. Once inside the network, the hacker leaked the username and password database.

Vulnerability: The vulnerabilities divided into two main issues: (1) the hacker was able to steal credentials; and, (2) the password database was not salted.

TECHNICAL IMPACTS

Data breach: There was a potential breach of confidentiality regarding company intellectual property; furthermore, a wave of brute force attacks was identified after this incident. In 2012, LinkedIn disclosed that six million passwords were stolen, but revised the number to 167 million in 2016.

Account hijacking: This breach led to account hijacking incidents in other services due to password reuse.

BUSINESS IMPACTS

Financial: The forensics investigation and post-incident expenses were an estimated $1 million. Additionally, a class-action lawsuit awarded a total of $1.25 million to victims who had a premium account during the 2012 breach.

Operational: The company issued two notifications to users to reset passwords—first in 2012 and again in 2016. In 2016, users who had an account in were forced to reset their passwords again.

Compliance: LinkedIn failed to adequately protect user data. This is a violation of local, national and European Union (EU) rules/regulations (e.g. GDPR). Infractions may result in penalties, including fines.

Reputational: LinkedIn was sued for the data loss, but didn't realize negative impacts on long-term service usage.

PREVENTATIVE CONTROLS

EKM-02: *Key Generation*—Employees must take good care of all access management tools, keys, passwords and cryptosystems.

IAM-12: *User ID Credentials*—The organization needs to take proper steps to verify identity, restrict access and maintain adherence to industry standards and compliance.

GRM-03: *Management oversight*—Leaders within the various corporate divisions (e.g. SOC, GRC, CIRT) had a clear responsibility to disclose the breach after detection. Under some United States sectoral regulations (e.g., the Sarbanes-Oxley Act [SOX]) , executive management could be held personally liable and receive fines or lose previously awarded bonuses.

GRM-06: *Policy*—It is unclear whether the LinkedIn policies were non-existent, deficient or simply not followed. Due to the severity of the breach, breach disclosure notification should not have been delayed.

DETECTIVE CONTROLS

IVS-01: *Audit logging / Intrusion detection*—Proper logging is required for legal and compliance reasons, along with incident response and forensics needs. This ensures a clear documentation of user actions in the case of an incident or intrusion.

IVS-06: *Network security*—The environment and infrastructure should be designed to restrict access and monitor traffic. This configuration should be verified and maintained with proper documentation.

SEF-04: *Incident response legal preparation*— Proper forensic procedures must be followed, especially if future criminal prosecution will take place. The inclusion of legal representation in incident response is important.

GRM-05: *Management support/involvement*—The fact a password change was only "recommended" for some users—and not forced on all users—indicates that management was either unaware of the scale of the problem or ignoring it.

GRM-10: *Risk assessments*—Any independent internal or external auditor should have tested the organization for appropriate incident response policy, processes and procedures. At some level, the disconnects between policy, reviews, support, oversight and/or incident cleanup must be uncovered and rectified.

TVM-02: *Vulnerability/patch management*— During a penetration test, passwords are typically tested for their strength using a variety of techniques (e.g. rainbow tables).

CORRECTIVE CONTROLS

SEF-01: *Contact/authority maintenance*—Including the applicable authorities and law enforcement in the initial incident response team would make the lack of disclosure a non-issue.

SEF-05: *Incident response metrics*—Metrics for accounting and future budget ramifications, including response time and resources spent, would bubble up through management and provide visibility to executive leadership.

GRM-08: *Policy impact of risk assessments*—The use of a risk-assessment feedback loop to better grasp the pitfalls of the initial breach would help avoid a second breach.

GRM-09: *Policy reviews*—Business leadership should take the lead in policy review, and ensure policies match organizational activities and strategic direction. Either the Chief Financial Officer (CFO) or Chief Counsel (legal) would designate an assignee to "sign on the bottom line"—especially in publicly traded companies where the U.S. Securities and Exchange Commission (SEC) and SOX compliance come into play.

GRM-07: *Policy enforcement*—Proper policy should be created and enforced uniformly. Employees should know they are responsible for their actions.

KEY TAKEAWAYS

– Always hash and salt databases containing user credentials
– Implement careful logging and behavioral anomaly analysis

MongoDB

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
Security Researcher	Unauthorized Access	**TT 2** Insufficient Identity, Credential and Access Management	**TT 1** Data Breach Loss of user credentials, PII.	**Financial** – Post-incident cost **Operational** – Restoration of files from backup data	**Preventative** – IAM-04 – HRS-09 **Detective** – TVM-02 – IAM-10
TT 6 Malicious Insider		**TT 3** Insecure Interfaces and APIs	**TT 8** Data Loss	**Compliance** – Loss of confidentiality of highly sensitve data **Reputational** – Reputational: Citizen confidence in the capabilities of their elected officials	**Corrective** – IAM-02 – IAM-06 – IAM-07 – IAM-09 – IAM-12 – HRS-09

ATTACK DETAILS

Threat actor: A threat actor could be any malicious actor who discovers an unprotected default installation of a MongoDB database.

Threat: A default installation the MongoDB database could be accessed without any authentication or access control when browsing the open MongoDB 27017 port issue. Cyber security expert Chris Vickery found data stored in an Amazon Web Services (AWS) MongoDB database—including personally identifiable information (PII) and voting records of 93 million Mexican voters—to be at-risk.

Vulnerability: An unsecured MongoDB port 27017 allowed an outside network attack, and no authentication or access control was enforced for the backend database MongoDB. All data could be manipulated (added, removed, modified and queried) by anyone.

TECHNICAL IMPACTS

Data breach: Data breaches can expose information to competitors, criminals, terrorists, rogue nation states and other malevolent users.

Data Loss: Data loss through destruction or deletion can make information unacceptable or unavailable to use for operations, analysis and decision making

BUSINESS IMPACTS

Financial: Hundreds of millions of dollars in audit spending, incident recovery, legal reimbursement and fines.

Operational: Operational impacts includes time and effort taken to restore files from backup data.

Compliance: A violation of state and federal regulations in the U.S. (including The Privacy Act), business-to-business (B2B) agreements and user-privacy obligations. Under Mexican law, voter data is classified as "strictly confidential," and unauthorized disclosure could be punished with a penalty of up to 12 years in prison.

Reputational: Data breaches may significantly damage a company's reputation. Utilization of MongoDB was widespread. In addition to the Mexican voter data exposure event, other organizational PII data breaches related to MongoDB likely impacted bottom lines as well.

PREVENTATIVE CONTROLS

IAM-04: *Policies and procedures*—The data owner is responsible for providing and implementing adequate policies and procedures on identification and access control for MongoDB data. This system should be established before the database is created and used to store information.

HRS-09: *Training/awareness*—The data owner should provide security awareness training for all contractors, third-party users and employees to ensure each person involved receives appropriate, timely instruction on policies and procedures (as mentioned in IAM-04).

DETECTIVE CONTROLS

IAM-10: *User access reviews*—The data owner should periodically review identity management and access rights to detect violations and make sure users are set to "least privilege" based on job function.

TVM-02: *Vulnerability/patch management*—A data owner conducting regular vulnerability scans and other checks would detect that assets are inadequately secured.

CORRECTIVE CONTROLS

IAM-02: *Credential Lifecycle/Provision Management*—The data owner is responsible at the application level to provide the authentication, authorization, and accounting (AAA) rules for access to data. This should be applied during the whole credential lifecycle.

HRS-09: *Training/awareness*—A security awareness training program should be provided for all contractors, third-party users and employees to ensure each stakeholder receives appropriate instruction. Timely educational updates on policies and procedures would also be beneficial, especially from an authentication and authorization perspective.

IAM-06: *Source code access restriction*—Application access controls for backend databases should be enforced, with access keys and credentials managed away from the source code. Integration, change management, implementation procedures and packaging could all enforce preventative, "least-privilege" access controls.

IAM-07: *Third-party access*—An application provider that consumes MongoDB services data should be considered a third-party access. Cloud Service Providers (CSPs) would be responsible for controls checking (such as access-control implementation) prior to service provisioning and access of the MongoDB service.

IAM-09: *User access authorization*—A data owner should provide and test appropriate user-access authorization. User-access authorization testing should easily catch the MongoDB default configuration in this case study.

IAM-12: *User ID credentials*—The data owner should restrict the internal corporate or customer (tenant) user-account credentials.

KEY TAKEAWAYS

– Security policy and preventative controls must be implemented across all perimeters
– Vulnerability and systems scanning for managed, shared and public environments is essential

Dirty Cow

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
Internal **External**	Undetectable Privilege Escalation (CVE-2016-5195)	**Operation** Insiders, External threat actors, untrained employees, weak governance **Operational** Flat or underdeveloped technical risk management framework **Operational** Absent, impaired, and/or incomplete telemetry over stand-alone or cloud container and/or virtualized images	**TT 4** System Vulnerability	**Financial** – Denial or theft of services, fraud, stock drop **Operational** – Disrupted operations, denial of service, theft of services **Compliance** – Fines, penalties, technical baseline, erosion **Reputational** – Brand damage	**Preventative** – AIS-02 – AIS-04 – IAM09 – IAM-12 – IAM-13 – HRS-02 **Detective** – CCC-03 – CCC-05 – GRM-10 – GRM-11 **Corrective** – BCR-01 – AAC-02

ATTACK DETAILS

Threat actor: A malicious internal or external person, group, or Advanced Persistent Threat (APT) seeking root-level control via an existing user account, weak vetting, or social engineering.

Threat: An unprivileged local user could use this flaw to gain write access to read-only memory, and escalate system privileges. Exploitation of this bug did not leave any trace of abnormal events within the system logs.

Vulnerability: Local privilege escalation could be used in conjunction with other exploits to execute non-privileged code and achieve a remote root shell.

TECHNICAL IMPACTS

System vulnerability: Exploitation of this vulnerability led to a race condition. This vulnerability exists in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3, allowing unprivileged local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping. This enables an attacker to escalate privileges on a Linux system.

BUSINESS IMPACTS

Financial: The financial impact can vary, depending on the type of system affected. Organizations are more liable to financial penalties stemming from infractions connected to the exposure, including: invalidated privacy covenants; data protection covenants; financial crimes (money laundering, fraud, account takeover); or trafficking in illicit goods and services.

Operational: Data and systems control loss create reduced assurances over data integrity, fidelity, lineage, and provenance—affecting the quality of business and operational decision-making capacity.

Compliance: Compliance violations can fall into sovereign and/or international scope, such as consumer, privacy, security, financial, and data-protection compliance violations.

Reputational: Financial losses, disrupted operations and compliance fines and penalties adversely affect brand value. As a result, doubts are raised about organizational management personnel and their ability to effectively oversee goals and responsibilities. This may also include a loss of consumer confidence and a diminished perception of brand quality.

PREVENTATIVE CONTROLS

AIS-02: *Customer access requirements*—Access grants must be implemented using a need-to-know, need-to-access protocol. Social engineering recognition training reinforces existing access management procedures to thwart account take-over—a precursor attack tree to a Dirty Cow event.

AIS-04: *Data security/integrity*—Multiple layered technical baselines contribute to data security across multiple system interfaces, jurisdictions, and business functions. Regular automated baseline assessments detect data and system disclosure, alteration, or destruction—thus reducing Dirty Cow risk potential. Baselines should include a known profile of expected production binaries, services, and processes. Reference monitoring or consistency maintenance runtime checks should be introduced to regularly assess nominal system behavior.

IAM-09: *User access authorization*—Dirty Cow risk potentials could be thwarted by disabling direct interactive login for maintenance and support. Additionally, settings could be configured to force image, container or Application Programming Interface (API) access through a cryptographically secured Jump Virtual Machine (VM) image or other cryptographic intermediary network enabled device.

IAM-12: *User ID credentials*—System administration function should be guarded by role-based entitlement, or two-factor/multi-factor authentication. Additionally, privileges should be separated between business-as-usual systems-level access, and escrowed credential access for sensitive root or system accounts.

IAM-13: *Utility program access*—Utility programs capable of potentially overriding system, object, network, virtual machine and application controls should be removed. If the attacker must load tooling on the system (assuming network anomaly detection is in place), the upload is a detectable event.

HRS-02: *Background screening*—All systems, contractors, and third-party contractors should undergo a background verification proportional to data classification (taking into account business requirements and acceptable risks). A Dirty Cow event can be perpetrated by an insider, which is an individual already trusted by the platform.

DETECTIVE CONTROLS

CCC-03: *Quality testing*—Follow a defined quality change control and testing process (e.g., Information Technology Infrastructure Library (ITIL) service management) with established baselines, testing and release standards that focus on system availability, confidentiality, and integrity of systems and services. Foreknowledge of production environment composition and behavior can alert staff to the presence of Dirty Cow-like anomalies.

CCC-05: *Production changes*—Manage risk potentials by documenting changes to: (1) business-critical or customer (tenant)-impacting applications (physical and virtual); (2) system-to-system interface (API) designs and configurations; and (3) infrastructure network and systems components.

GRM-10: *Risk assessments*—Lower Dirty Cow risks through a three-line, enterprise-wide, risk-management framework. Formal, first-line technical risk assessment occurs at planned intervals and in conjunction with any changes to information systems. Second-line risk determines the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risks should be determined independently, and by considering all risk categories.

GRM-11: *Risk management framework*—Mitigate all Dirty Cow risk potentials to an acceptable level; this process should be based on risk criteria that adheres to the "risk appetite" boundaries established by the organization.

CORRECTIVE CONTROLS

AAC-02: *Independent audits*—Develop recurring, first-line technical risk assessment programs specific for Dirty Cow threat models that demonstrate a higher residual operational risk than what can be mitigated with available controls, processes, and technologies.

BCR-01: *Business continuity planning*—Establish a testable and consistent unified framework for business continuity planning and development. Consider cross-functional, table-top exercises for Dirty Cow threat models that demonstrate a higher residual operational risk than what can be mitigated with available controls, processes, and technologies.

KEY TAKEAWAYS

– Social engineering training needs to remain aligned with account takeover tactics
– Perform recurring automated activity baselines from different perspectives

Zynga

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
Internal Disgruntled Employee **TT 6** Malicious Insider	Business and Sensitive Data Theft	**TT 2** Insufficient Identity, Credential and Access Management	**TT 1** Data Breach	**Financial** – Forensics & legal investigations and action costs **Operational** – Allocation of time and resources for an investigation **Compliance** – Potentially in violation of SOX **Reputational** – Reputational loss – Loss of competitive advantage – Loss of trade secrets	**Preventative** – AIS-03 – AIS-04 – IAM-05 – HRS-03 – SEF-03 – DSI-01 – ASI-04 **Detective** – AIS-04 – IAM-11 – DSI-02 **Corrective** – IAM-11 – SEF-04 – SEF-05

ATTACK DETAILS

Threat actor: An internal, disgruntled Zynga employee/team leader (a malicious insider) in research and development.

Threat: The malicious insider downloaded highly confidential business documents—in accord with his designated access rights and the need-to-know-principle—and removed them from a company laptop (and premises) before "defecting" to a competitor.

Vulnerability: No document-level data loss prevention controls were applied; no security controls alerted a distributed bulk folder/file download from the company cloud storage; and no physical data loss prevention controls were practiced.

TECHNICAL IMPACTS

Data breach: Exposure of business documents and product documentation.

BUSINESS IMPACTS

Financial: The competitor who obtained Zynga's insider knowledge probably reaped considerable business and technological competitive advantages. For Zynga, this likely resulted in diminished long-term income, as well as a decrease in stock value.

Operational: Zynga was forced to allocate time and resources for an investigation (technical, legal and operative alike). Additionally, business strategies and product roadmaps will require new development strategies.

Compliance: Weak controls associated with the data theft are potentially in violation of the Sarbanes-Oxley Act, and could have resulted in fines.

Reputational: Client and partners are more hesitant to trust Zynga with their confidential information, thereby hindering the company's product adoption and ability to disrupt markets.

PREVENTATIVE CONTROLS

AIS-03: *Data integrity*—Controls employed to prevent bulk and/or selective "output" (a "download" in this case) would force the attacker to resort to a print screen strategy, or employ an otherwise ineffective technique.

AIS-04: *Data security/integrity*—Separate policies and procedures can be implemented for outgoing employees

IAM-05: *Segregation of duties*—Segregating access to confidential data on a need-to-know basis—as well as restricting copy/download privileges—would go far in limiting a data breach loss.

HRS-03: *Employment agreements*—Employees must understand their legal obligations to the company, both while they are employed and after they depart.

SEF-03: *Incident reporting*—The capacity to report incidents is critical, both to deter potential offenders and to empower whistle blowers. Previous insider data breach case studies convey the importance of strong organizational incident reporting mechanisms when it comes to attack deterrence. If attackers perceive these mechanisms to be strong, and are aware that sensitive data are routinely scrutinized and responsibly managed by the data owner, attacks are less likely to occur.

DSI-01: *Classification*—Classify data and restrict access appropriately.

AIS-04: *Data security/integrity*—For organizations seeking to shield themselves from inherent risks, it is an essential first step for data owners to understand exactly what data are processed, stored and transmitted in their infrastructure (or cloud, as it may be), as well as the applications that are being utilized.

DETECTIVE CONTROLS

AIS-04: *Data security/integrity*—Audit log and detective controls should be established to enable forensics to proactively detect data leaks, both reducing time to respond and limiting loss.

IAM-11: *User access revocation*—Exiting employees with access to highly privileged data should have their access revoked in a timely manner (in accordance with an organization's policies and procedures).

DSI-02: *Data inventory/flows*—Data Loss Prevention (DLP) solutions—such as one integrated in a cloud productivity suit or enforced on transit or endpoints—could detect data leakage based on content, context or an advanced behavioral analytics/artificial intelligence (AI) scenario, even if such action is permissible by policy.

CORRECTIVE CONTROLS

IAM-11: *User access revocation*—In this case, the perpetrator had access appropriate to their job and data needs. Many cases of insider threats manifest after employment termination, primarily due to negligence in access revocation.

SEF-04: *Incident response legal preparation*—The implementation of employee Non-Disclosure Agreements, formal awareness action and corresponding legal action in response to a breach of terms can produce partial loss recovery, loss mitigation and insurance coverage.

SEF-05: *Incident response metrics*—Insurance can provide protection against data and/or business/trade secrets loss, and a partial recovery of a loss in the case of Intellectual Property theft.

KEY TAKEAWAYS

– Data loss prevention and detective controls are imperative
– Security and data privacy awareness is the primary preventive control

Net Traveler

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
External	**Open Spear Phishing Email** (CVE-2012-0158)	**Insiders** (Untrained, Neglectful, Malicious) **Applications-Operations** (Outdated Version & Patching) **Applications-Security** (Outdated Version & Patching	**TT 1** Data Breach **TT 8** Data Loss	**Financial** – Lost Revenue – Additional Expense **Operational** – Disrupted Operations – Affected Decision Making **Compliance** – Fine – Penalties **Reputational** – Reduced Brand Value	**Preventative** – TVM-01 – TVM-02 – HRS-09 **Detective** – AAC-01 – AAC-02 – AAC-03 **Corrective** – SEF-01 – SEF-02 – BCR-11

ATTACK DETAILS

Threat actor: An external group sought access to a targeted system for obtaining information, spreading disinformation and affecting system operations.

Threat: The external group sent a spear phishing e-mail to an employee containing either: (1) a URL link to a site containing RAR-executables, or (2) Word attachments built with MNKits that deliver an executable payload. Opening the file leads to Net Traveler exploiting a weakness in Microsoft (MS) Windows Common Controls ActiveX (MSCOMCTL.OCX), allowing a remote attacker to execute arbitrary code on the system with the privileges of the victim.

Vulnerability: Employees who are not properly trained to recognize and deal with phishing attacks are potential victims. Furthermore, systems must be sufficient hardened (e.g. patching, anti-virus) in order to prevent successful attacks.

TECHNICAL IMPACTS

Data breach: Data breaches can make production information available to competitors reducing a company's competitive advantage. In some cases, military intelligence may also be made available to terrorists (i.e. rogue nation states), placing a nation's security at-risk.

Data loss: Data loss through destruction or deletion can make information unacceptable or unavailable to use for operations, analysis and decision making.

BUSINESS IMPACTS

Financial: Data breaches may result in reduced competitive bid sales as well as GDPR fines and penalties. Corrupted/lost data may result in inefficient, ineffective analyses and poor decision making—translating to reduced sales and extra costs.

Operational: Data unavailable or unusable for processing transactions, analysis and decision making can disrupt operations and delay and/or affect the quality of the decision-making process. Data obtained by competitors can reduce competitive advantage.

Compliance: Data improperly gathered, handled or disclosed (breach) can result in violations of local, national and international rules/regulations (e.g., GDPR).

Reputational: Financial losses, disrupted operations and GDPR compliance fines and penalties can affect brand value. As a result, confidence about organizational management personnel—and their ability to oversee the company's security and other responsibilities—is undermined.

PREVENTATIVE CONTROLS

TVM-01: *Anti-virus/malicious software*—Supporting business processes and technical measures should be implemented to ensure the installation of updated anti-virus software. This will prevent the execution of malware on connected endpoint devices (i.e., workstations, laptops, and mobile devices), as well as IT infrastructure network and systems components.

TVM-02: *Vulnerability/patch management*—Supporting business processes and technical measures should be implemented that ensure vulnerability/patch maintenance is up-to-date. This will allow for timely detection of vulnerabilities within organizationally owned or managed applications, as well as with infrastructure network and system components—ensuring the efficiency and effectiveness of security controls.

HRS-09: *Training/awareness*—Security and privacy awareness training programs must be established for all employees, contractors and third-party users connected with the organization. All individuals with access to organizational data must receive appropriate security and privacy awareness training, as well as regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.

DETECTIVE CONTROLS

AAC-01: *Audit planning*—Audit plans must be developed and maintained to address business process disruptions. Auditing plans need to focus on reviewing the efficiency and effectiveness of the implementation and continuous performance of security/operations—including versioning, patching and security/privacy training.

AAC-02: *Independent audits*—Independent reviews and assessments must be performed (at least annually) to promote best practices and ensure the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations. Independent and internal audits need to be coordinated to ensure efficient and effective coverage of operations, including versioning, patching and security/privacy training.

AAC-03: *Regulatory mapping*—Organizations must create and maintain a control framework which captures standards, as well as regulatory, legal, and statutory requirements relevant to their business needs. The control framework, including controls over versioning, patching and security/privacy training, needs to be reviewed (at least annually) to ensure changes that could affect the business processes are reflected.

CORRECTIVE CONTROLS

SEF-02: *Incident management*—Policies and procedures must be established, and supporting business processes and technical measures implemented, to triage security related events and ensure timely and thorough incident management (as established per IT service management policies and procedures).

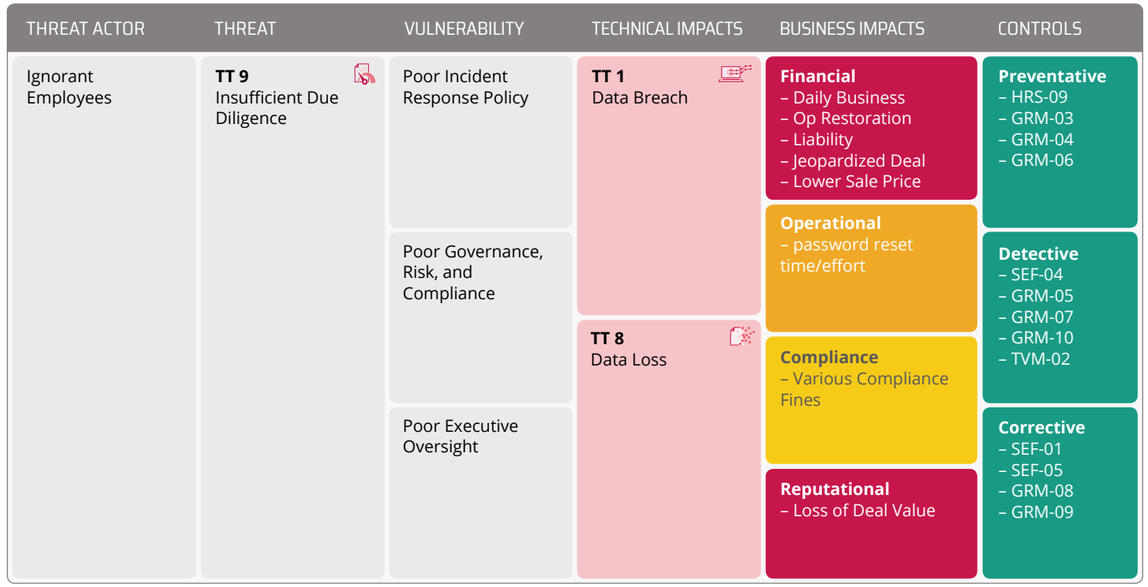
SEF-03: *Incident reporting*—Workforce personnel and external business partners must be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all security events in a timely manner. Security events needs to be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, and regulatory compliance obligations.

BCR-11: *Retention policy*—Backup and recovery measures must be incorporated and tested as part of business continuity planning. Backup and recovery needs to be invoked based on a review of threat's impact (i.e. corrupt, damaged or deleted data or systems).

KEY TAKEAWAYS

– Train insiders to remain vigilant and skeptical when opening e-mails
– Timely implementation of the latest application/OS patches/versions is critical

Yahoo!



ATTACK DETAILS

Threat actor: Multiple employees downplayed, ignored or were possibly unaware of two different breach incidents.

Threat: The initial attack included poor password security, specifically due to using MD5 hashing past its period of usefulness.

Vulnerability: The Yahoo! staff showed a lack of proper due diligence at multiple levels. This included: (1) the incident response policy did not include breach notification; (2) the Governance, Risk management and Compliance (GRC) management program did not recognize/report the breaches as a risk to future operations; and (3) executives ignored the risks associated with the situation for upwards of three years.

TECHNICAL IMPACTS

Data breach: There is a potential breach of confidentiality by attackers regarding company intellectual property. Such information could include source code, trade secrets or other highly sensitive information. Beyond the breach, there are possibilities of data corruption, but this was not evidenced in the Yahoo! case. Another significant headline from the breach included the theft of 500 million usernames/passwords.

Data loss: Due to delayed disclosure and consumer username/password reuse, the data loss rippled across the industry. Internal security teams across the world tested the Yahoo! password lists against their directories, finding reuse prevalent and forcing widespread password resets.

BUSINESS IMPACTS

Financial: Depending on which systems were compromised, financial expenses associated with the breach were likely significant for the company—ranging from daily business/sales losses to operational restoration costs. Most visibly, the disclosures jeopardized a pending Verizon acquisition bid in 2016. While the purchase was later finalized, the final sales price was reduced by an estimated $350 million for breach-related reasons.

Operational: The impact of the breach wasn't just felt by Yahoo!: The entire computing industry felt operational impacts due to the sheer volume of passwords potentially reused.

Compliance: Yahoo! is responsible for 50 percent of any cash liabilities incurred related to non-SEC government investigations, as well as third-party litigation connected to the breaches. Furthermore, liabilities arising from shareholder lawsuits and SEC investigations will continue to be the responsibility of Yahoo!.

Reputational: The breach and delayed disclosure raised questions internally and publicly, specifically regarding the strategic value of Verizon's acquisition of the company and the significance of the price/cost of resolving the security problems. There have been numerous shareholder lawsuits.

PREVENTATIVE CONTROLS

HRS-09: *Training/awareness*—Yahoo! employees at multiple levels would benefit from security awareness training. This situation should bump against every division within the organization, including: legal, human resources (HR), risk and compliance and security. All these departments need to understand the impact of this event.

GRM-03: *Management oversight*—Leaders within the SOC, IT, GRC and CIRT divisions had a clear responsibility to disclose information after detecting both intrusions.

GRM-04: *Management program*—The policy, communications and risk management aspects of an Information Security Management Program (ISMP) were lacking or ignored by Yahoo!. Documentation, approval and implementation all create artifacts for later detective and corrective actions.

GRM-06: *Policy*—It is unclear whether the Yahoo! policies were non-existent, deficient or simply not followed. Due to the severity of the breach disclosure notification should not have been delayed.

DETECTIVE CONTROLS

SEF-04: *Incident response legal preparation*— Proper forensic procedures must be followed, especially if future criminal prosecution will take place. The inclusion of legal representation in incident response is important.

GRM-05: *Management support/involvement*—Deciding not to blow the whistle at any point suggests a cultural problem within the organization. Ignoring/covering up a complication, or not defining clear protocols related to accountability and responsibility should be considered red flags.

GRM-07: *Policy enforcement*—Information security policy enforcement actions, including additional training or disciplinary steps, should ensure successful policy implementation. While Verizon may have analyzed documented policies during the acquisition process, due diligence would suggest reviewing the enforcement records to verify that said documents were not simply "for show."

GRM-10: *Risk assessments*—Any independent internal or external auditor should catch breaches of this magnitude as going unreported. At some level, the disconnects between policy, reviews, support, oversight and/or incident cleanup must be uncovered and rectified.

TVM-02: *Vulnerability/patch management*— During a penetration test, passwords are typically tested for their strength using a variety of techniques (e.g. rainbow tables).

CORRECTIVE CONTROLS

SEF-01: *Contact/authority maintenance*—Including the applicable authorities and law enforcement in the initial incident response team would make the lack of disclosure a non-issue.

SEF-05: *Incident response metrics*—Metrics for accounting and future budget ramifications, including response time and resources spent, would bubble up through management and provide visibility to executive leadership.

GRM-08: *Policy impact on risk assessments*—The use of a risk-assessment feedback loop to better grasp the pitfalls of the initial breach would help avoid a second breach.

GRM-09: *Policy reviews*—Business leadership should take the lead in policy review, and ensure policies match organizational activities and strategic direction. Either the Chief Financial Officer (CFO) or Chief Counsel (legal) would designate an assignee to "sign on the bottom line"—especially in publicly traded companies where the SEC and SOX compliance come into play.

KEY TAKEAWAYS

– There is no long-term benefit in not disclosing incidents, unless directed by police
– Weak password and authentication mechanisms are easily replaced with Multi-Factor Authentication (MFA) tokens

Zepto

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
Ignorant Employee	**TT 8** Data Loss	**Operating System Policy** – Windows icons	**TT 1** Data Breach	**Financial** – Daily Business – Op Restoration – Liability – Ransom Payment	**Preventative** – HRS-08 – HRS-09 – TVM-01 – IAM-05
		Software Policy – Collaboration programs		**Operational** – File restoration time/ effort – Business Continuity Support	**Detective** – HRS-05 – TVM-03 – SEF-02 – SEF-04
	TT 10 Abuse & Nefarious Use of Cloud Services		**TT 8** Data Loss	**Compliance** – Various Compliance Fines – Disclosure Notice Costs	
		Inadequate Employee Training		**Reputational** – Loss of Competitive Advantage – Remediation Expenses	**Corrective** – SEF-01 – BCR-02 – BCR-10 – SEF-05

ATTACK DETAILS

Threat actor: An ignorant employee opened a spam message with a ".wsf" or ".docm" file attachment.

Threat: The .wsf file included detection evasion scripts combining multiple programming languages, allowing it to pass through emulation engines that rely on a single language. The malicious file also used sharing and collaboration in Software as a Service (SaaS) cloud services—including Microsoft OneDrive, Google Drive, Box and Dropbox—to infect other systems.

Vulnerability: Windows changes a .wsf file icon to look like a valid spreadsheet file. Furthermore, collaboration software made the .wsf file look like a local file to employees with inadequate training.

TECHNICAL IMPACTS

Data breach: There was a potential breach of confidentiality by attackers regarding company intellectual property. Such information could include source code, trade secrets or other highly sensitive information. This is most likely not the case for Zepto, although the attackers did have access to some sensitive data. Combing through the files for sensitive data patterns (i.e., PII, social security numbers (SSN), and credit card numbers (CCN)) could be accomplished with minimal effort.

Data loss: After encryption, all files were unavailable until backup restoration or key retrieval.

BUSINESS IMPACTS

Financial: Depending on which systems were compromised, financial expenses associated with the breach were likely significant for the company—ranging from daily business/sales losses to operational restoration costs. Recent events also suggest that some organizations may pay the ransom. This practice is highly discouraged, as proceeds simply fund better ransomware attack vectors (see NoMoreRansom.org).

Operational: Operational impacts include the time and effort taken for file backup restoration.

Compliance: Compliance impacts could include fines and liabilities, such as disclosure notices or penalties levied by regulators.

Reputational: The affected organization might suffer reputational blows if there is an external loss of service access. Such impacts are visible and noticeable to the organization's customers and the general public. Breach notifications can severely damage an organization's reputation, especially for organizations in specific industries/locations.

PREVENTATIVE CONTROLS

HRS-08: *Technology acceptable use*—The integration of various cloud services should be an architectural activity and not left up to individual users/groups for implementation. The choice of storage vendors must be made by corporate IT/security. Failing to do so might mean that specific customer-identified risks are not being addressed.

HRS-09: *Training/awareness*—Ransomware is most effectively distributed through e-mail in phishing/spear-phishing attacks. Security awareness training for employees will reduce the risk of employees falling victim to such attacks.

TVM-01: *Anti-virus/malicious software*—Security providers continue making advances in malware detection and protection. Even the most well-trained employees can benefit from such tools being implemented.

IAM-05: *Segregation of duties*—Proper segregation of duties limits the "blast radius" of nefarious activities by cordoning off business-critical data sets from the larger populace. Additionally, sectioning off groups within the business-critical sets, by function or organization, impedes the spread of malware to the entire network.

DETECTIVE CONTROLS

HRS-05: *Mobile Device Management*—Employee phishing training is less effective on mobile devices, as information is hidden and presented on a smaller screen. As a result, due diligence (i.e., checking links) is less intuitive. Tighter controls on app deployment and integration could prove useful to offset the drawbacks of mobile devices.

TVM-03: *Mobile code*—Protection and controls for execution and interaction on mobile devices could disallow .wsf file interactions with the mobile device.

SEF-02: *Incident management*—The incident response team should be charged with immediate cleanup, and may consider disconnecting SaaS storage as part of the remediation process.

SEF-04: *Incident response legal preparation*— Proper forensic procedures must be followed, especially if future criminal prosecution will take place. The inclusion of legal representation in incident response is important.

CORRECTIVE CONTROLS

HRS-05: *Mobile Device Management*—Employee phishing training is less effective on mobile devices, as information is hidden and presented on a smaller screen. As a result, due diligence (i.e., checking links) is less intuitive. Tighter controls on app deployment and integration could prove useful to offset the drawbacks of mobile devices.

TVM-03: *Mobile code*—Protection and controls for execution and interaction on mobile devices could disallow .wsf file interactions with the mobile device.

SEF-02: *Incident management*—The incident response team should be charged with immediate cleanup, and may consider disconnecting SaaS storage as part of the remediation process.

SEF-04: *Incident response legal preparation*— Proper forensic procedures must be followed, especially if future criminal prosecution will take place. The inclusion of legal representation in incident response is important.

KEY TAKEAWAYS

– Educate users on the importance of security, especially file attachments and links
– Remain vigilant on patching and updating endpoint protection definitions

DynDNS

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
External Malicious	Distributed Denial of Service	**TT 2** Insufficient Identity, Credential and Access Management	DNS Resolution Failure	**Financial** – Daily Business – Op Restoration – Loss of existing clients	**Preventative** – IVS-13 – AAC-01 – GRM-01
		External IoT Devices Connected		**Operational** – Internet was down for several hours – Business Continuity Support	**Detective** – SEF-04
		Hacking of MIRAI Botnet	**TT 11** Denial of Service	**Compliance** – Service level agreement compliance	**Corrective** – BCR-01 – BCR-02 – BCR-10 – TVM-01
		Inadequate mechanisms to identify earlier		**Reputational** – Loss of Competitive Advantage	

ATTACK DETAILS

Threat actor: Malicious externals targeted attacks through connected IoT devices, causing a Distributed Denial of Service (DDoS) in October 2016.

Threat: The mastermind behind the attack utilized Mirai malware to infect IoT devices to create a botnet. The botnet was then used to launch the DDoS attack.

Vulnerability: IoT devices were compromised due to the use of default credentials. These compromised devices were then incorporated into a botnet. This botnet was later configured to launch the DDoS attack on Dyn, a domain name system (DNS) provider. Customers of Dyn who did not have a backup DNS provider were impacted, as DNS queries to their sites couldn't be resolved.

TECHNICAL IMPACTS

Denial of service: The attack spanned a range of domains managed by Dyn, indicating that interrupting Dyn's services was the goal. The DDoS attack strength on Dyn's systems was documented at 1.2 Terabytes per second (Tbps)—considered at the time to be the most powerful attack on record. The core result was that DNS failed to translate into a proper Internet Protocol (IP) addresses, giving the appearance that Dyn services were down.

BUSINESS IMPACTS

Financial: There were two major fallouts from the incident. (1) For Dyn clients: Downtime resulted in business losses, as did the cost of restoring downed domains. These figures, however, are difficult to calculate. (2) For Dyn: There were operational restoration costs and a loss of various, important clients. These details, however, were not reported.

Operational: Key client domains were unreachable, including Twitter and Snapchat.

Compliance: There is no direct compliance impact for Dyn, as their data were not compromised. For companies that used Dyn's services, there may have been service-level agreement (SLA)-related compliance issues, given the downtime duration.

Reputational: While this attack was not due to a fault or vulnerability in Dyn's system, the company's reputation was impacted nonetheless. The primary responsibility for this incident rests with the IoT device manufacturers and owners—as well as the protocol design of domain name services.

PREVENTATIVE CONTROLS

IVS-13: *Network architecture*—The design of architecture should include quick identification, isolation and re-route as part of a defense against a DDoS attacks.

AAC-01: *Audit planning*—Plans should be established for auditing the internal network and customer endpoints. A regular, random audit of the connected IOT devices is also suggested. This could also include malware identifications on the customer side as well.

GRM-01: *Baseline requirements*—It is important to clearly document proper system response baselines for components. In the Dyn case study, this principally included routers and DNS servers (which are impacted heavily in the case of DDoS attacks). Regular monitoring and review of compliance guidelines should be documented to detect any unidentified changes in the system. This process can provide early identification of a DDoS attack.

DETECTIVE CONTROLS

SEF-03: *Incident reporting*—A clear process for incident reporting should be documented, and personnel should be trained to respond quickly and effectively.

CORRECTIVE CONTROLS

BCR-01: *Business continuity planning*—Business continuity planning should establish a clear response system in case of a DDoS or network seizure. The plan should prioritize network restoration as quickly as possible to minimize disruptions.

BCR-02: *Business continuity testing*—The business continuity plan (BCP) should include simulation for DDoS-type attacks to effectively test service-restoration response times. Specific internal DDoS attacks could be organized for test purposes, though testing on a public Cloud Service Provider must be requested in advance for obvious reasons.

BCR-10: *Policy*—Policies should address stakeholder preparedness for emergency scenarios within an organization, and standard operating procedures should be adhered to (as per organizational policies and procedures).

TVM-01: *Anti-virus/malicious software*—Although the Dyn DNS attack was principally applied to consumer IoT cameras, organizations should establish policies and procedures to prevent the execution of malware on organizationally owned or managed-user endpoint devices.

KEY TAKEAWAYS

– Maintain awareness of Internet of Things (IoT) issues and analyze network traffic for anomalies
– Properly review, validate and test business continuity plans and monitor system uptime

Cloudbleed

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
External Malicious	**TT 1** Data Breach	**TT 12** Shared Technology Vulnerabilities	Memory Leakage	**Financial** – None	**Preventative** – EKM-03 – IVS-09
				Operational – Forced credential resets – Credential leakage	**Detective** – TVM-02 – CCC-03
	Loss of Confidentiality	Buffer Overrun Vulnerability	Failure/Lack of Isolation	**Compliance** – Sensitive Data Leakage	**Corrective** – TVM-02 – IAM-12
				Reputational – Loss of customer trust	

ATTACK DETAILS

Threat actor: An external malicious actor could send HyperText Transfer Protocol (HTTP) requests to Cloudflare's vulnerable services. The vulnerability was dubbed "Cloudbleed."

Threat: To trigger the vulnerability, the following requirements had to be met: (1) the final buffer had to finish with a malformed script or .img tag; (2) the buffer had to be less than 4KB in length; (3) the customer had to have either e-mail obfuscation enabled or automatic HTTPS rewrites/server-side excludes in combination with another feature that utilized the old parser; and (4) the client IP must have a poor reputation.

Vulnerability: In a buffer over-read vulnerability, more memory was returned to the requester than was desired, resulting in memory leakage. Furthermore, Cloudflare is a shared technology, so the vulnerability affects more than just one tenant in a cloud service.

TECHNICAL IMPACTS

Denial of service: Leakage of API keys, passwords and other credentials are possible.

Isolation failure: This results in queries to Cloudflare returns dumped memory from any of its customers.

BUSINESS IMPACTS

Financial: The incident created minimal service disruptions for Cloudflare, and any bigger impacts to Cloudflare customers were undisclosed.

Operational: Operational impacts included the time and effort taken to reset passwords; additionally, credentials may have been exposed.

Compliance: Sensitive information, such as PII data or health records, could have been leaked due to Cloudbleed. A breach of confidentiality of such data usually leads to compliance impacts, such as fines or investigations. Fortunately, there were no reported incidents related to this Cloudbleed attack.

Reputational: Cloudflare probably experienced some reputational impacts for a security company, as the vulnerability led to a loss in confidentiality for their customers.

PREVENTATIVE CONTROLS

EKM-03: *Sensitive data protection*—Sensitive data should be protected via encryption. In the event of a data leak, the sensitive information will not be disclosed.

IVS-09: *Segmentation*—Data segmented and protected according to sensitivity levels will provide more protection during a data leak.

DETECTIVE CONTROLS

TVM-02: *Vulnerability/patch management*—Cloud Service Providers should inform customers of the extent to which data were exposed and what customers can do to protect themselves.

CCC-03: *Quality testing*—Cloud Service Providers should conduct regular testing of service to discover and re-mediate vulnerabilities in a timely manner.

CORRECTIVE CONTROLS

TVM-02: *Vulnerability/patch management*—Cloud Service Providers should inform customers of the extent to which data were exposed and what customers can do to protect themselves.

IAM-12: *User ID credentials*—Affected customers should immediately force password or credential resets for affected systems.

KEY TAKEAWAYS

– Vulnerabilities within an organization's supply chain still impact organizational risk
– Cloud tenant segmentation depends on implementation, and is not absolute

References

LINKEDIN

- https://motherboard.vice.com/en_us/article/53ddqa/linkedin-finally-finished-resetting-all-the-passwords-leaked-in-2012
- https://www.rferl.org/a/us-charges-russian-hacker-nikulin-stealing-date-linkedin-san-francisco-dropbox-formspring-/28068596.html
- https://www.rferl.org/a/russia-hacker-prague-identity-nikulin/28065492.html
- https://www.computerworld.com/article/3077478/security/linkedin-s-disturbing-breach-notice.html
- https://arstechnica.com/tech-policy/2016/10/linkedin-says-hacking-suspect-is-tied-to-breach-that-stole-117m-passwords/

MONGODB

- http://www.informationweek.com/cloud/infrastructure-as-a-service/93-million-mexicanvoter-database-exposed-on-amazon-cloud/d/d-id/1325259
- https://www.csoonline.com/article/3018592/security/database-configuration-issues-expose-191-million-voter-records.html
- https://www.silvertech.com/blog/2017/march/how-to-secure-mongodb-and-get-the-most-out-of-the-sitecore-experience-platform
- https://securityaffairs.co/wordpress/46588/data-breach/mexican-voter-records.html

DIRTY COW

- https://www.scmagazineuk.com/researchers-call-bull-on-dirty-cow-patch-find-flaw/article/711799/
- https://www.theguardian.com/technology/2016/oct/21/dirty-cow-linux-vulnerability-found-after-nine-years
- https://en.wikipedia.org/wiki/Dirty_COW
- https://access.redhat.com/security/vulnerabilities/DirtyCow
- https://www.infoworld.com/article/3134888/linux/how-bad-is-the-dirty-cow-linux-kernel-vulnerability.html
- https://www.cvedetails.com/cve/CVE-2016-5195/

ZYNGA

- https://www.documentcloud.org/documents/3227518-Zynga-Case.html#document/p3/a329534
- https://arstechnica.com/tech-policy/2016/11/zynga-sues-2-former-employees-over-alleged-massive-data-heist/
- https://www.databreaches.net/zynga-sues-2-former-employees-over-alleged-massive-data-heist/

NET TRAVELER

- https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-a4.pdf - Page 18 - Advanced Persistent threats – NetTraveler APT Targets Russian, European Interests
- https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests
- http://researchcenter.paloaltonetworks.com/2016/01/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/
- https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-office-exploit-generators-szappanos.pdf

YAHOO!

- https://en.wikipedia.org/wiki/Yahoo!_data_breaches
- https://www.leahy.senate.gov/imo/media/doc/9-27-16%20Yahoo%20Breach%20Letter.pdf
- http://fortune.com/2016/12/19/yahoo-hack-cyber-security/
- http://www.nbcnews.com/tech/tech-news/your-yahoo-account-was-probably-hacked-company-set-confirm-mass
- http://www.reuters.com/article/us-yahoo-cyber-idUSKBN14420S
- http://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement
- http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-inhistory.html
- https://www.usatoday.com/story/tech/news/2017/02/21/verizon-shaves-350-million-yahoo-price/98188452/

ZEPTO

- https://www.netskope.com/blog/zepto-variant-locky-ransomware-delivered-via-popular-cloud-storage-apps/
- https://www.tripwire.com/state-of-security/latest-security-news/the-newest-online-threat-zepto-ransomware/
- https://nakedsecurity.sophos.com/2016/07/05/is-zepto-ransomware-the-new-locky/
- http://niiconsulting.com/checkmate/2016/08/zepto-ransomware-analysis-and-how-to-protect-yourself/

DYNDNS

- https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
- https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
- https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/
- https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html

CLOUDBLEED

- https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/
- https://www.troyhunt.com/pragmatic-thoughts-on-cloudbleed/
- https://en.wikipedia.org/wiki/Tavis_Ormandy