SECURE YOUR GOOGLE WORKSPACE

A Guide To Data Breach Prevention

Strategies And Best Practices For Safeguarding Your Google Workspace Environment

GAT labs

Table of Contents

CHAPTER 1

The Evolving Landscape of Cyber Threats

1.1. Phishing Attacks:

A Persistent Threat in Today's Cyber Threat Landscape

Phishing remains one of the most prevalent cyber threats, involving deceptive emails designed to trick users into divulging sensitive information or clicking on malicious links.

The Rising Tide of BEC Attacks

Business Email Compromise (BEC) is a severe form of phishing targeting specific individuals, often mimicking executives or trusted partners. Attackers exploit this trust to manipulate victims into transferring funds or revealing sensitive information.

For example, in 2019 Japan's Toyota Boshoku Corporation was hit with a **$37 million BEC attack.** Due to the company's size, the amount might seem staggering, but hackers were able to trick an employee into transferring the funds from the European subsidiary before detection.

Defending Against Phishing Attacks

To protect against phishing attacks, use a multi-layered approach:

- **Advanced Email Security:** Deploy solutions that use machine learning to filter out phishing emails. GAT+ helps admins quickly remove these emails from all accounts.
- **Employee Training:** Regularly educate staff on phishing tactics and run simulations to improve awareness.
- **Strong Passwords:** Require complex passwords and consider using password managers.
- **Multi-Factor Authentication (MFA):** Implement MFA to add an extra security layer, making unauthorized access harder.
- **Incident Response Plan:** Develop and maintain a plan to quickly address and manage phishing incidents.

CHAPTER 1

The Evolving Landscape of Cyber Threats

1.2. Ransomware:

A Growing Cyber Threat

Ransomware encrypts files and demands payment for decryption, with evolving tactics such as:

- **Crypto-ransomware:** This is the most common form of ransomware, where attackers encrypt files using strong encryption keys, making them inaccessible without the decryption key.
- **Locker ransomware:** This type of ransomware locks the entire system, preventing access to all files and applications.
- **Double extortion:** Beyond encrypting files, attackers also steal data and threaten to expose it publicly if the ransom is not paid.

Researchers reported an 18% year-on-year increase in ransomware attacks, with healthcare, manufacturing, and technology sectors being the hardest hit by cybercrime gangs.
The Colonial Pipeline attack serves as a stark reminder of the devastating consequences of ransomware. The pipeline, which supplies fuel to much of the East Coast of the United States, was forced to shut down after a ransomware attack, leading to fuel shortages and economic disruption.

Mitigating the Ransomware Threat

To defend against ransomware, implement a layered approach:

- **Regular Backups:** Ensure robust, offline backups are stored securely and tested regularly.
- **Employee Training:** Educate staff on ransomware, phishing, and the dangers of suspicious emails.
- **Network Segmentation:** Isolate critical systems to limit ransomware spread.
- **Regular Software Updates:** Keep software updated with the latest security patches.
- **Incident Response Planning:** Develop and regularly update a plan for containment, recovery, and communication.

CHAPTER 1

The Evolving Landscape of Cyber Threats

MSPs: The Gateway to Ransomware

Managed Service Providers (MSPs) often serve as entry points for ransomware attacks due to their management of IT services across multiple clients. A compromised MSP can grant attackers access to numerous client networks, amplifying the impact of their attacks. Thus, securing MSP environments is crucial to preventing widespread ransomware incidents.

The recovery process can be extremely costly; IBM's Cost of a Data Breach Report 2024 estimates **the global average cost of a data breach at USD 4.88 million**—a 10% increase from the previous year and the highest total ever. This figure includes costs related to data restoration, system repairs, and implementing enhanced security measures.

Avoid paying the ransom whenever possible, as there's no guarantee of recovery and it may incentives further attacks. A strong preventive strategy and a well-defined incident response plan are key to reducing ransomware risk and impact.

1.3. Insider Threats:
A Hidden Danger

Insider threats, originating from within an organization, present a unique challenge. These threats can be intentional or accidental but are often just as damaging.

Understanding Insider Threats

Insider threats can arise from various sources, including:

- **Employees:** Current or former staff with access to sensitive information.
- **Contractors:** Temporary workers with access to systems.
- **Privileged Users:** Individuals with elevated permissions, such as IT admins.

Motivations behind insider threats range from financial gain and revenge to negligence or disruption.

CHAPTER 1

The Evolving Landscape of Cyber Threats

Mitigating Insider Threats

To manage insider threats effectively, consider a comprehensive strategy:

- **Employee Screening and Onboarding:** Perform thorough background checks and robust onboarding.
- **Access Controls:** Implement the principle of least privilege, giving access only as needed for job functions.
- **Data Classification:** Categorize data by sensitivity to determine access levels.
- **User Monitoring:** Use User and Entity Behavior Analytics (UEBA) to spot unusual activities.
- **Incident Response Planning:** Develop a plan for investigating, containing, and recovering from insider threats.
- **Employee Education:** Regularly train employees on data protection and the implications of insider threats.

By implementing these measures, organizations can better protect themselves from the complex and often subtle risks posed by insiders.

CHAPTER 1

The Evolving Landscape of Cyber Threats

1.4. Zero-Day Exploits:

The Invisible Threat

Zero-day exploits are vulnerabilities unknown to software vendors, allowing attackers to exploit them before patches are available. Despite continuous updates from providers like Google Workspace, the rapid discovery and exploitation of these vulnerabilities highlight the need for robust mitigation strategies.

The Impact of Zero-Day Exploits

Successful zero-day attacks can lead to:

- **Data Breaches:** Unauthorized access to sensitive information before a patch is deployed.
- **System Compromise:** Gaining control over systems and networks.
- **Financial Loss:** Operational disruptions and recovery costs.
- **Reputational Damage:** Harm to an organization's public image following a breach.

Mitigating Zero-Day Risks

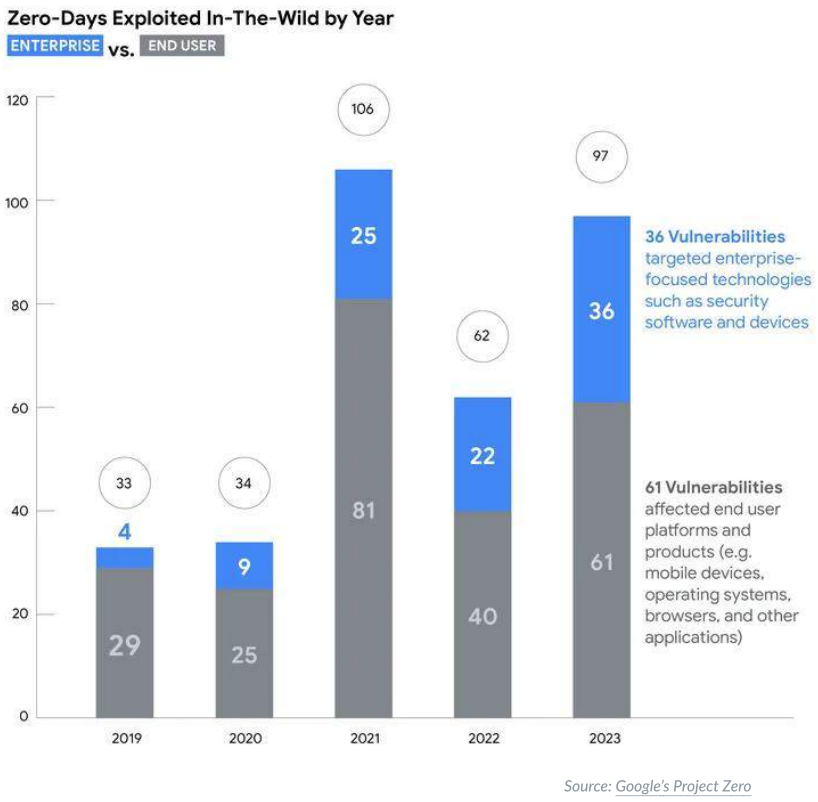
To reduce the impact of zero-day exploits:

- **Software Updates:** Regularly update software and operating systems to include the latest patches.
- **Employee Training:** Educate staff on the risks of phishing and unsafe downloads.
- **Threat Intelligence:** Keep up with emerging threats and vulnerabilities.
- **Incident Response Planning:** Prepare a plan for responding to breaches.
- **Network Segmentation:** Isolate critical systems to contain potential damage.

CHAPTER 1

The Evolving Landscape of Cyber Threats

According to Google's Project Zero, 2023 saw a significant rise in zero-day vulnerabilities, with a record 97 zero-day vulnerabilities exploited in-the-wild. That's over 50 percent more than in 2022, but still shy of 2021's record of 106. The average time to patch a zero-day vulnerability remains critical, as unpatched exploits can remain a threat for months.



Source: Google's Project Zero

That's why, implementing these strategies can help organizations strengthen their defenses and better manage the risks associated with zero-day exploits.

CHAPTER 1

The Evolving Landscape of Cyber Threats

1.5. Malware and DDoS Attacks:

Understanding the Dual Threat

Malware and Distributed Denial of Service (DDoS) attacks are among the most persistent threats in cybersecurity. While they function differently, they can be interrelated, with malware often enabling DDoS attacks.

Malware: The Silent Infiltrator

Malware, or malicious software, infiltrates systems to steal data, disrupt operations, or cause damage. Common types include:

- **Viruses:** Self-replicating programs that spread through infected files.
- **Worms:** Self-propagating malware that spreads across networks without user interaction.
- **Trojans:** Malicious programs disguised as legitimate software.
- **Spyware:** Software that secretly collects user data.

According to the Cybersecurity Ventures report, the global annual cost of cybercrime is predicted to reach **$9.5 trillion USD in 2024.**

DDoS Attacks: Overwhelming the System

DDoS attacks flood a target with traffic to make it unavailable. They often leverage botnets—networks of compromised devices—to generate massive traffic volumes.

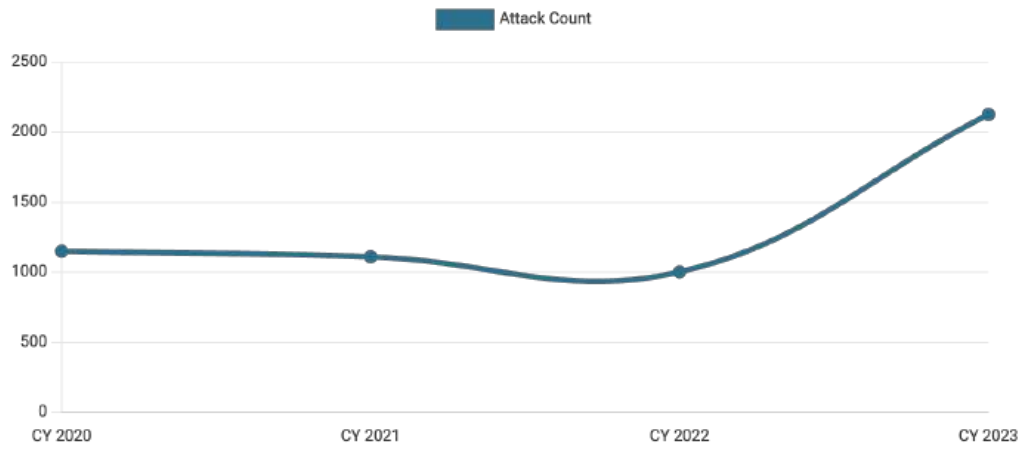
How DDoS Attacks Work:

- **Botnets:** Attackers use networks of infected devices to launch coordinated attacks, overwhelming the target.
- **Service Disruption:** The targeted system slows down or crashes, denying service to legitimate users.

CHAPTER 1

The Evolving Landscape of Cyber Threats

According to a report, DDoS attacks more than doubled in 2023, rising from just over 1,000 incidents in 2022 to over 2,100 in 2023. This significant increase underscores the growing threat that DDoS attacks pose to organizations globally.



Protecting Your Data Against Malware and DDoS Attacks

For Malware:

- **Keep Software Updated:** Regularly apply patches to address vulnerabilities.
- **Use Antivirus Software:** Deploy reliable antivirus programs to detect and remove malware.
- **Be Cautious with Email Attachments:** Avoid opening suspicious emails or links.
- **Educate Employees:** Train staff to recognise phishing and other social engineering tactics.
- **Backup Data Regularly:** Protect against data loss with frequent backups.

For DDoS Attacks:

- **DDoS Mitigation Services:** Employ services to detect and block malicious traffic.
- **Scalable Resources:** Use cloud-based solutions to handle large traffic volumes.
- **Firewalls and Intrusion Detection Systems (IDS):** Implement these to filter and detect malicious traffic.
- **Traffic Filtering:** Block traffic from suspicious IP addresses or regions.

CHAPTER 1

The Evolving Landscape of Cyber Threats

1.6. Data Breach Prevention Checklist (RECAP)

Regular Backups

- Ensure all critical data is backed up regularly and stored securely offline.
- Test backup systems periodically to confirm data recoverability.

Employee Training

- Conduct regular security awareness training on phishing, ransomware, and social engineering.
- Run simulations to test employee responses to potential threats.

Access Controls

- Apply the principle of least privilege, restricting access based on job roles.
- Regularly review and update access permissions for all users.

Software Updates

- Keep all systems, applications, and firmware up-to-date with the latest security patches.
- Enable automatic updates where possible.

Multi-Factor Authentication (MFA)

- Require MFA for all sensitive accounts and administrative access.
- Regularly review MFA logs for any suspicious activity.

Incident Response Plan

- Develop and maintain a comprehensive incident response plan.
- Conduct regular drills to ensure preparedness and efficiency.

DDoS and Malware Protection

- Implement DDoS mitigation services and scalable resources.
- Deploy reliable antivirus software and conduct regular scans.

CHAPTER 2

Implementing Strong Access Controls:

The Foundation of Data Security

Strong access controls are essential for any robust data security strategy. By restricting access to sensitive information and resources—such as disabling Hangouts and Meet chat/calls for end-users—organizations can greatly reduce the risk of data breaches.

2.1. The Principle of Least Privilege

The principle of least privilege ensures that users are only granted the minimum level of access necessary to perform their job functions. By adhering to this principle, organisations can minimise the potential damage from unauthorised access.

According to the 2024 Verizon Data Breach Investigations Report, **74% of data breaches involve the human element**, including misused credentials and weak access controls.

2.2. Implementing Effective Access Controls

1. **Strong Password Policies**
- Enforce the use of complex, unique passwords for all accounts.
- Consider implementing password managers to help employees securely manage their credentials.

2. **Multi-Factor Authentication (MFA)**
- Require MFA for all user accounts to add an extra layer of security.
- MFA significantly reduces the risk of unauthorized access, even if a password is compromised.
- GAT Shield enhances this security by enforcing MFA policies and monitoring login attempts.

CHAPTER 2

Implementing Strong Access Controls:

The Foundation of Data Security

3. **Role-Based Access Control (RBAC)**
- Define user roles clearly and assign permissions based on these roles.
- RBAC helps ensure that users only have access to the resources necessary for their roles.

4. **Regular Access Reviews**
- Conduct periodic reviews of user access levels to ensure they remain appropriate.
- GAT Labs simplifies this process by providing detailed access reports and automated alerts, allowing administrators to quickly identify and adjust discrepancies.
- Regular reviews help maintain the principle of least privilege and reduce the risk of data breaches caused by outdated or excessive access rights.

5. **Data Classification**
- Categorize data based on its sensitivity to determine appropriate access levels.
- This ensures that sensitive information is only accessible to those who need it.

92% reported exposure of sensitive data, with a majority acknowledging being harmed by the data exposure, as reported by the Cloud Security Alliance.

2.3. Securing Mobile Devices

With the rise in mobile device usage for work, it's crucial to implement security measures to protect data on these devices.

1. **Mobile Device Management (MDM)**
- Enforce security policies across all mobile devices used within the organization.
- Use MDM tools to remotely wipe lost or stolen devices to prevent data breaches.

2. **Data Encryption**
- Encrypt sensitive data stored on mobile devices to protect it from unauthorized access.

CHAPTER 2

Implementing Strong Access Controls:

The Foundation of Data Security

2.4.The Cost of Poor Access Controls

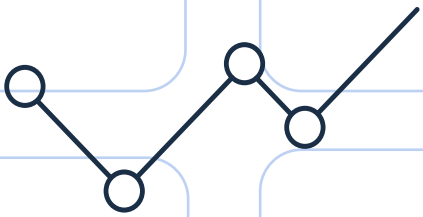
Poor access controls can lead to significant financial losses. Here are some key statistics that highlight the impact:

USD 4.88M

The global average cost of a data breach in 2024—a 10% increase over last year and the highest total ever. (IBM Cost of a Data Breach Report 2024)

Breach Costs Up 30% YoY

45% of organizations experienced a data breach due to weak access controls, leading to a 30% increase in breach costs year-over-year. (2024 Thales Data Threat Report)



90% of Orgs at Risk from Cloud Misuse

Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data. (Gartner)

44% of Experts Recommend IAM

Security Experts believe that their current security vulnerabilities can be addressed by implementing an Identity and Access Management (IAM) solution. (Expertinsights)

Strong access controls not only enhance security but also improve **compliance with regulations.** Organizations with robust access management practices are **40% more likely to achieve full compliance** with these regulations, reducing the risk of fines.

CHAPTER 3

Data Classification and Protection:

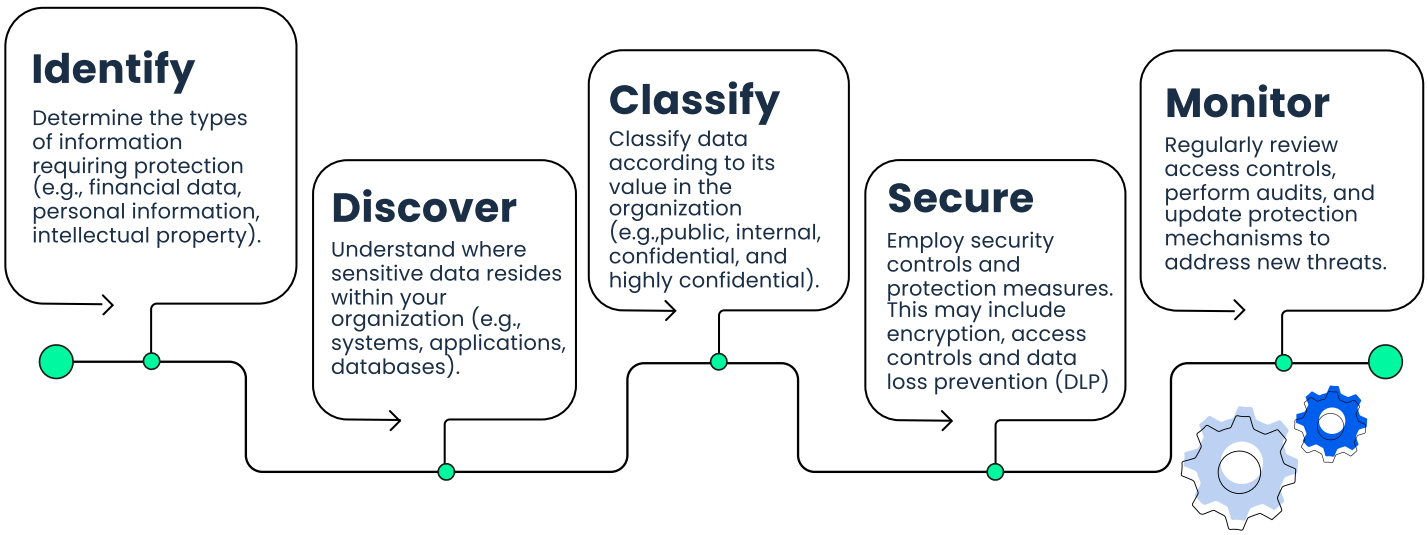
Safeguarding Sensitive Information

Effective data classification is essential for protecting sensitive information and preventing breaches within your Google Workspace environment. By categorizing data based on its value and sensitivity, you can apply the appropriate protection measures to ensure its security.

3.1. Data Classification Framework

To establish a comprehensive data classification system, follow these steps:

1. **Identify Sensitive Data:** Determine which types of information need protection, such as financial data, personal information, and intellectual property.
2. **Discover Data Locations:** Identify where sensitive data resides within your organization—this includes systems, applications, and databases.
3. **Create Classification Levels:** Develop clear categories based on data sensitivity, such as confidential, highly confidential, and public.
4. **Assign Ownership:** Designate responsible parties for managing and protecting each data category.
5. **Implement Labelling:** Consistently label data with the appropriate classification levels to ensure everyone knows how to handle it.



CHAPTER 3

Data Classification and Protection:
Safeguarding Sensitive Information

3.2. Data Protection Measures

Once data has been classified, apply the following protection measures:

1. **Access Controls:** Restrict access to sensitive data based on its classification level. Ensure that only authorized personnel can access high-risk information.

2. **Data Encryption:** Encrypt sensitive data both at rest and in transit to protect it from unauthorized access.

3. **Data Loss Prevention (DLP):** Utilize DLP tools to monitor and prevent data leakage. GAT Labs offers DLP solutions that help safeguard your Google Workspace data effectively.

   Tip: Regularly review and update DLP policies to adapt to evolving threats.

4. **Regular Data Backups:** Maintain regular backups of critical data to mitigate the risks associated with data loss. Ensure that backups are stored securely and tested for recoverability.

According to the 2024 Veeam Data Protection Trends report that **70% of organizations will use cloud-powered data protection services by 2026.**

Why It Matters

Implementing a robust data classification and protection framework not only reduces the risk of unauthorized access but also ensures compliance with regulatory requirements, such as GDPR and CCPA. A well-executed classification system helps prioritize protection efforts, making it easier to secure the most critical information within your organization.

CHAPTER 4

Incident Response Planning:
Prepare for the Worst

A well-structured incident response plan (IRP) is crucial for mitigating the impact of a data breach. By anticipating potential threats and establishing clear procedures, organizations can respond effectively, minimize damage, and recover swiftly.

4.1. Key Components of an Incident Response Plan

Incident Identification and Reporting

- Establish clear protocols for identifying and reporting potential incidents.
- Encourage employees to promptly report any suspicious activity.

Incident Response Team

- Assemble a dedicated team responsible for managing incidents, including representatives from IT, security, legal, and communications.
- Ensure that each team member understands their role and responsibilities during an incident.

Communication Plan

- Develop clear communication channels for internal and external stakeholders.
- Include guidelines for media relations and regulatory reporting to manage public perception and compliance requirements.

Tip: Prepare communication templates in advance to expedite the process during an actual incident.

Investigation and Containment

- Outline steps for investigating the incident and containing the threat to prevent further damage.
- Focus on isolating affected systems and limiting the scope of the breach.

CHAPTER 4

Incident Response Planning:
Prepare for the Worst

Evidence Preservation

- Implement procedures for collecting and preserving digital evidence.
- Proper evidence handling is essential for legal actions and post-incident analysis.

Eradication

- Develop strategies for removing malware or other malicious code from the system.
- Ensure that eradication steps do not affect evidence preservation or system recovery.

Recovery

- Plan to restore systems and data to normal operations as quickly and safely as possible.
- Prioritize critical systems and ensure that all patches and updates are applied before bringing systems back online.

Organizations with a well-rehearsed recovery plan reduce their breach-related costs by 27%, according to The 2024 IBM Cost of a Data Breach Report

Post-Incident Analysis

- Conduct a thorough review of the incident to identify lessons learned.
- Use the findings to improve future responses and update the incident response plan accordingly.

Tip: Schedule a post-incident review within 30 days of the incident to ensure insights are fresh and actionable.

CHAPTER 4

Incident Response Planning:
Prepare for the Worst

4.2. Conducting Incident Response Simulations

Regularly testing your incident response plan is critical to ensure that it remains effective and relevant. Simulations help identify weaknesses and improve response capabilities.

Tabletop Exercises

- Discuss potential scenarios and test response procedures in a low-pressure environment.
- Use these exercises to evaluate team understanding and preparedness.

Live Simulations

- Simulate real-world incidents to evaluate team performance under pressure.
- Live simulations help build muscle memory and reveal practical challenges that might not be apparent in tabletop exercises.

By investing time and resources in incident response planning and simulations, organizations can significantly enhance their ability to manage and recover from security incidents, ultimately reducing the impact of breaches on their operations and reputation.

CHAPTER 5

How to Prevent Data Breaches: Regular Security Audits

Regular security audits and assessments are crucial for identifying vulnerabilities and ensuring the effectiveness of your data protection measures. By conducting thorough evaluations, you can proactively address potential data breaches and maintain a high level of security in your Google Workspace environment.

5.1. Types of Security Audits

1. **Vulnerability Assessments**
- Identify weaknesses in systems, applications, and networks before they can be exploited.

Tip: Schedule these assessments regularly, especially after major updates or changes to your infrastructure.

2. **Penetration Testing**
- Simulate cyberattacks to assess your organizations's security posture.

3. **Compliance Audits**
- Verify adherence to industry regulations and standards, such as GDPR and CCPA.

Tip: Use these audits to identify gaps in your compliance efforts and address them proactively.

4. **Risk Assessments**
- Evaluate potential threats and their impact on the organization.
- Regular risk assessments help prioritize security efforts based on the most significant threats to your organization.

The 2023 Global Risk Management Study found that organizations with regular risk assessments were **50% more likely to avoid major security incidents.**

CHAPTER 5

How to Prevent Data Breaches:
Regular Security Audits

5.2. Incorporating SIEM for Enhanced Security Audits

A key component of regular security audits is leveraging tools that provide comprehensive visibility into your security environment. One such tool is Security Information and Event Management (SIEM). SIEM solutions collect and analyze security data from various sources—such as logs, applications, and devices—to provide real-time monitoring, alerting, and reporting.

Benefits of SIEM:

- **Centralized Data Collection:** SIEM aggregates logs and events from across your Google Workspace environment and other systems into one platform for easier management.
- **Real-Time Monitoring:** SIEM provides continuous, real-time monitoring of security events, enabling faster detection and response to potential threats.
- **Advanced Threat Detection:** SIEM solutions use behavioral analytics, machine learning, and correlation rules to identify anomalies and alert you to unusual activities, such as unauthorized access attempts or data exfiltration.
- **Compliance Reporting:** SIEM simplifies the process of meeting regulatory requirements (e.g., GDPR, HIPAA, CCPA) by providing detailed reports and audit trails.
- **Incident Response Support:** SIEM platforms help your incident response team by providing clear insights into the scope of an attack, helping streamline investigation and recovery processes.

In a Google Workspace environment, where logs and events come from various sources like Gmail, Drive, and third-party apps, SIEM can centralize these logs and identify suspicious patterns that might be overlooked otherwise.

CHAPTER 5

How to Prevent Data Breaches:
Regular Security Audits

5.3. IDS and IPS for Threat Prevention

In addition to SIEM, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play critical roles in securing your Google Workspace environment:

- **Intrusion Detection Systems (IDS):** IDS identifies and monitors malicious activities or policy violations within your network, alerting your security team when potential threats are detected.

- **Intrusion Prevention Systems (IPS):** IPS takes IDS a step further by not only detecting potential threats but actively preventing or blocking attacks before they can cause damage.

IDS vs IPS – Key Differences

- **IDS:** Identifies attacks and alerts the security team but does not stop the attack itself.
- **IPS:** Proactively blocks attacks in real time, preventing them from breaching your systems.

Why Use IDS/IPS in Google Workspace Audits?

- **Proactive Protection:** IPS stops attacks before they infiltrate, making it a key tool for reducing the risk of successful breaches.

- **Comprehensive Monitoring:** IDS provides detailed logs and alerts, which can be analyzed through SIEM systems for broader insights into potential threats and vulnerabilities.

- **Incident Response:** Both IDS and IPS work together to enhance incident response efforts by identifying threats early and preventing them from escalating.

CHAPTER 5

How to Prevent Data Breaches:
Regular Security Audits

5.3. Benefits of Regular Audits

1. **Identify Vulnerabilities**
- Uncover weaknesses before they can be exploited by attackers.

2. **Demonstrate Compliance**
- Ensure your organization meets regulatory requirements, reducing the risk of fines and legal issues.

3. **Enhance Security Posture**
- Implement corrective measures based on audit findings to strengthen defenses.

4. **Build Confidence**
- Reassure stakeholders, including customers and partners, about your organization's commitment to security.

Incorporating Audits into Your Security Strategy

By integrating regular security audits into your overall strategy, you establish a continuous improvement cycle that helps maintain a high level of protection for your Google Workspace environment.

Explore our Google Workspace Auditing Hub for expert blogs and detailed guidance on various audit types. Or, download our "10-Step Guide to Auditing Google Workspace" directly here.

CHAPTER 5

How to Prevent Data Breaches:
Regular Security Audits

5.4. Next Steps:
Building a Resilient Security Posture

Employee Training and Awareness

- Ongoing education on security best practices is crucial. Regular training sessions help employees recognize threats like phishing and social engineering.
- Incorporate real-world scenarios into training to enhance learning outcomes.

Third-Party Risk Management

- Assess the security practices of vendors and partners to ensure they meet your security standards. GAT+ provides an application risk assessment so you can judge whether a company has a valid reason for a privilege given. *SEE MORE HERE*

Incident Response Testing

- Regularly simulate security incidents to evaluate your organization's preparedness.

Leveraging Advanced Technologies

- Explore AI, machine learning, and automation for threat detection and response.

Regular security audits and assessments are the backbone of a resilient security posture. By incorporating these practices into your organization's security strategy, you can proactively identify and address vulnerabilities, ensure compliance, and build confidence among stakeholders.

CHAPTER 6

Additional Resources

For deeper insights and more comprehensive information on data breach prevention and Google Workspace security, explore the following resources:

- 10 Essential Steps to Audit Your Google Workspace
- Data Compliance in Google Workspace
- Cybersecurity & Infrastructure Security Agency (CISA)
- Cybersecurity Incident Response Plan Template
- Monitoring Google Cloud Login Behavior with GAT+

By leveraging these resources, you'll gain valuable knowledge and best practices to strengthen your organization's security posture and effectively prevent data breaches.

CHAPTER 6

Final Thoughts: Preventing Data Breaches

Preventing data breaches in Google Workspace is a complex challenge that demands a multifaceted approach. By understanding the evolving threat landscape, implementing robust security controls, and fostering a culture of cyber resilience, organizations can significantly enhance their ability to protect sensitive information.

Remember, data security is an ongoing process. Stay informed about emerging threats, regularly review and update your security measures, and encourage employees to remain vigilant. By adopting a proactive approach, you can build a strong security posture that safeguards your organization's valuable assets.

6.1. Next Steps to Strengthen Cybersecurity:

- **Conduct a Comprehensive Security Audit:** Identify vulnerabilities and prioritize remediation efforts.
- **Implement Advanced Threat Detection and Response Solutions:** Stay ahead of emerging threats.
- **Provide Ongoing Security Awareness Training:** Empower employees as your first line of defense.
- **Partner with a Cybersecurity Expert:** Assess your organization's risk profile and develop a tailored security strategy.

By taking these steps, you can significantly reduce the risk of data breaches in your Google Workspace environment and ensure the security of your organisation's most valuable data.

Dive Deeper Into GAT Labs

EXPLORE MORE

VISIT OUR WEBSITE

SCHEDULE A DEMO

15 DAY FREE TRIAL

GAT labs