What are Cyber Security Solutions?
Cyber security solutions are technological tools and services that help protect organizations against cyber attacks, which can result in application downtime, theft of sensitive data, damage to reputation, compliance fines, and other adverse consequences.

In the modern security environment, with a wide variety of ever-changing threats, tools are an essential part of cybersecurity. We'll review several broad categories of cyber security solutions:

Application security solutions—help test software applications for vulnerabilities during development and testing stages, and protect them against attacks when running in production.
Endpoint security—deployed on endpoint devices like servers and employee workstations, prevent threats like malware and unauthorized access and help detect and stop breaches as they happen.
Network security—monitor network traffic, identify potentially malicious traffic, and enable the organization to block, filter, or otherwise mitigate threats.
Internet of things (IoT) security—help gain visibility and apply security controls to the growing network of IoT devices, which are increasingly used for mission-critical applications and store sensitive data, yet are often unsecured by design.
Cloud security—help gain control over complex public, private, and hybrid cloud environments, by detecting security misconfigurations and vulnerabilities, and helping to remediate them.
What are Enterprise Security Solutions?
Enterprise security solutions help enterprises enforce security policies across their infrastructure.

What Is Enterprise Security Management?
Enterprise security management (ESM) is the practice of implementing security policies for the purpose of protecting complex ecosystems. ESM encompasses the configuration, deployment, and monitoring of security policies across several environments and security tools.

The goal of ESM is to enable enterprises to gain better control over a distributed and complex enterprise environment. Enterprises can leverage ESM to address unauthorized access concerns, as well as to meet privacy and compliance requirements.

ESM protects both data at rest and data in transit. Enterprises can use ESM to protect information as it passes through various connections, devices, and environments, including personally-owned devices, distributed systems, and cloud infrastructure.

Typically, the enterprise leadership team is responsible for leading ESM efforts, including the CISO, CIO, and CSO. Ideally, their ESM efforts should help protect the enterprise against external and internal threats, including internal threats.

What Is Enterprise Security Governance?
An enterprise security governance plan helps organizations define a roadmap that helps fulfill regulatory requirements, control risk, and manage security operations.

Ideally, an enterprise security governance framework aligns business goals and compliance objectives with the mission and vision of the organization.

Enterprise security management is often practiced in accordance with the overall enterprise security governance strategy.

Here are several notable governance frameworks:

Control Objectives for Information and Related Technologies (COBIT) – provides best practices to help align business requirements with technology.
Information Technology Infrastructure Library (ITIL) – outlines best practices to help enterprises align business requirements with IT services.
International Organization for Standardization (ISO) 27001– defines requirements for implementing information security management.
National Institute of Standards and Technology (NIST) – provides several cybersecurity frameworks.
Application Security
Application security processes and tools help organizations discover, fix, and continuously remediate application security threats. To be truly effective, application security should be applied at all levels—including software and hardware.

A router, for example, can help prevent unauthorized traffic from penetrating the network, and a vulnerabilities scanner can help discover and remediate vulnerabilities before a breach occurs. Together, they protect different components of the application.

Web Application Firewall (WAF)
WAF is a policies-based filter located in front of a web application and audits the HTTP/S traffic moving between

the Internet and the application. A WAF attempts to detect and prevent malicious threats and activities.

API Security
Application programming interfaces (APIs) enable communication between different applications. Since this process lets you transfer information between services and applications, it is highly vulnerable to interceptions. API security solutions help protect APIs and prevent exploitations of transmissions or vulnerabilities.

DDoS Protection
A denial-of-service (DoS) attack attempts to interrupt the normal operations of a single server or an entire network. If the attack is successful, the targeted device, application, or network suffers from an outage or disruption that prevents normal operations. A distributed denial-of-service (DDoS) attack typically targets websites. DDoS protection can help prevent disruptions during attacks.

Software Composition Analysis (SCA)
Software Composition Analysis (SCA) solutions analyze the open-source components of your application. After the SCA identifies open-source software, the tool provides information about each library, including licensing information and data on detected security vulnerabilities. Enterprise versions of SCA often provide additional capabilities, such as automated policies.

Application Security Testing (SAST/DAST/IAST)
Here are the three main approaches to application security testing:

Static Application Security Testing (SAST)—tools that use white-box testing to inspect static source code and provide reports on security issues. You can leverage SAST to check non-compiled code for syntax and math errors, and to run binary analyzers on compiled code.
Dynamic Application Security Testing (DAST)—tools that use black-box testing to inspect code in runtime and provide information about potential security vulnerabilities, such as leakage, authentication, data injection, and query strings. You can use DAST to simulate a large number of scenarios.
Interactive Application Security Testing (IAST)—tools that leverage both DAST and SAST approaches to discover a wider range of vulnerabilities. IAST tools are deployed in the application server, where they dynamically inspect compiled source code during runtime.
Runtime Application Self-Protection (RASP)—tools that leverage IAST, DAST, and SAST, and can detect and prevent a greater range of security threats. RASP tools can analyze user traffic and application traffic during runtime, for example. Once threats are detected, RASP tools can actively respond to the event.
Data Security
Here are key categories of data security tools.

Sensitive Data Management
Sensitive data management solutions help organizations identify and manage various types of sensitive data, including:

Personally identifiable information (PII)
Payment card industry (PCI) data
Protected health information (PHI)
Intellectual property (IP)
Sensitive data management solutions typically integrate with multiple systems, ensuring organizations can manage sensitive information spread across different applications, databases, and user endpoints.

Data Compliance
Data compliance processes help organizations ensure that protected information is properly organized, managed, and handled according to the relevant regulatory requirements. This typically starts with identifying the data type and then implementing the appropriate security and privacy measures. Organizations may use more than one solution to achieve compliance, including tools that automatically identify data types.

Threat Prevention
Threat prevention solutions help organizations detect and prevent known advanced threats and vulnerabilities. This process often involves filtering and distributing relevant data to several tools, which provide further assistance, response, and analysis.

Data Governance
Data governance processes help organizations manage the entire data lifecycle. The goal is to maintain data availability, integrity, and usability. A data governance solution provides capabilities that help organizations define policies and processes, specify data owners, and effectively control and manage data movement.

Cloud Discovery
Cloud discovery tools help organizations identify cloud instances running during a certain point in time. This includes applications, containers, databases, and any other cloud-based component. The goal is to provide organizations with a centralized view of all cloud components, including information about data, storage, and performance. Typically, cloud discovery tools provide auto-discovery capabilities that work across multi-cloud

environments.

Endpoint Security
Here are the most common endpoint security solutions.

Endpoint Protection Platform (EPP)
EPP tools provide point-in-time protection. Once files enter the network, the APP tool scans it and looks for known threats. Traditional antivirus (AV) solutions, for example, scan files while looking for known signature-based threats.

Endpoint Detection and Remediation (EDR)
EDR solutions provide active protection by proactively and continuously monitoring all files and applications entering a device. EDR solutions provide granular visibility and analysis and detect a range of threats, rather than just signature-based attacks. For example, EDR can detect ransomware, fileless malware, polymorphic attacks, and more.

Extended Detection and Response (XDR)
XDR solutions provide extended protection and response across multiple layers of security. Typically, XDR involves a stack of tools and capabilities that leverage intelligent analysis and automation when performing threat detection and response. This enables XDR solutions to provide more visibility and collect and correlate a huge amount of threat data.

Cloud Infrastructure Security
Here are popular cloud infrastructure security tools.

Cloud Access Security Brokers (CASB)
Cloud Access Security Broker (CASB) solutions are implemented as a security layer running between a cloud provider and the corporate network. The CASB extends visibility and enables organizations to monitor and secure access to their data.

Cloud Workload Protection Platform (CWPP)
A cloud workload protection platform (CWPP) is a solution that helps secure server workloads running in a public cloud infrastructure as a service (IaaS) environment. A CWPP helps organizations ensure that workloads remain secure while passing through multiple public cloud environments. The main advantage of CWPP is managing several environments through a single console.

Cloud Security Posture Management (CSPM)
Cloud Security Posture Management (CSPM) is the practice of using several strategies and tools to manage and orchestrate security across cloud services and resources. CSPM solutions provide the tools needed to manage cloud security, including tools for compliance, monitoring, logging, reporting, and incident detection and response. You also gain automation capabilities for a wide range of tasks.

Network Security
Here are major categories of network security tools:

Network access control—enables organizations to control and restrict access to the network. Notable features include denying network access to non-compliant devices, placing devices in quarantined areas, and restricting access to resources.
Network segmentation—enables organizations to control traffic flow. You can, for example, use network segmentation to stop all traffic in one network area from reaching another, and limit the flow of traffic according to source, type, and destination.
Network-Based IDS (NIDS)—solutions designed to monitor an entire network. NIDS tools provide visibility into all traffic that flows through the network. The tool can make determinations according to packet metadata and contents and can detect threats. However, NIDS tools do not provide endpoint-level visibility.
Next-generation firewalls (NGFW)—designed to secure the connections between the network, firewall, and the Internet. NGFW solutions typically use static and dynamic packet filtering, VPN support, whitelists, and signature-based IPS when enforcing security.
Internet of Things (IoT) Security
Here are three important IoT security technologies:

IoT network security—helps you secure network connections between IoT devices and back-end systems. This usually requires antivirus software, antimalware, firewalls, and intrusion detection, and prevention.
IoT encryption—helps you mask data at rest and in transit as it moves between IoT edge devices and back-end systems. This usually requires the use of cryptographic algorithms and managing the encryption key lifecycle.
IoT authentication—helps users securely authenticate and use their IoT devices. This requires managing multiple users per device and providing authentication mechanisms, such as static passwords, multi-factor authentication, and biometrics.
Emerging Cyber Security Solution Trends
DMARC

Domain-based message authentication, reporting, and conformance (DMARC) is an authentication protocol built especially for email communication. The DMARC protocol uses the sender policy framework, (SPF) and DomainKeys identified mail (DKIM) to authenticate email messages.

DMARC adds another layer of trust, supporting the overall security efforts of the organization. You can add DMARC to supplement your security effort but note that it does not provide full coverage.

Passwordless Authentication
Passwordless authentication enables organizations to replace passwords with other forms of authentication, such as password generators, biometric signatures, and tokens. The goal is to reduce the amount of weak passwords created by users and prevent users from using their personal passwords for work purposes. Passwordless authentication can improve both security and user experience.

Zero Trust Cybersecurity
Zero trust is a security model that enforces strict access controls. The goal is to ensure that not only the traditional security perimeter is covered, but also all corporate assets distributed throughout various locations.

A laptop connected to the network, a mobile device connected to the corporate cloud, a SaaS environment shared with external parties—all of these should be treated with zero trust. At the most basic level, this means applying strict authentication across granular user types. Organizations also leverage endpoint security to enforce zero trust.

Privacy-Enhancing Computation
Privacy-enhancing computation can enable organizations to protect private information. A crucial goal here is to provide a trusted environment for processing sensitive data. Additionally, privacy-enhancing technologies typically leverage privacy-aware machine learning (ML) algorithms to decentralize data processing and analytics.

Privacy-enhancing computation often involves the use of homomorphic encryption—a type of cryptography that lets third parties process encrypted data. The third party then returns only encrypted results to the owner of the data, without providing information about the results or data. This process lets collaborators share data without breaching privacy.

Hyper Automation
Hyper automation is the practice of automating as many IT and business processes as possible. This typically involves the use of several decision processes and automation technologies, such as artificial intelligence (AI), machine learning (ML), and robotic process automation. The goal is to help organizations reduce the overhead and inefficiencies associated with legacy systems by creating efficient, automated, and interconnected pipelines.

Cyber Security Solutions with Imperva
Imperva provides a holistic cybersecurity solution that comprehensively covers application security and data security. Imperva integrates with your Security Information and Event Management (SIEM) system to enable integration with other cybersecurity solutions covered in this post.

Imperva Application Security Solutions
Imperva provides comprehensive protection for applications, APIs, and microservices:

Web Application Firewall – Prevent attacks with world-class analysis of web traffic to your applications.

Runtime Application Self-Protection (RASP) – Real-time attack detection and prevention from your application runtime environment goes wherever your applications go. Stop external attacks and injections and reduce your vulnerability backlog.

API Security – Automated API protection ensures your API endpoints are protected as they are published, shielding your applications from exploitation.

Advanced Bot Protection – Prevent business logic attacks from all access points – websites, mobile apps and APIs. Gain seamless visibility and control over bot traffic to stop online fraud through account takeover or competitive price scraping.

DDoS Protection – Block attack traffic at the edge to ensure business continuity with guaranteed uptime and no performance impact. Secure your on premises or cloud-based assets – whether you’re hosted in AWS, Microsoft Azure, or Google Public Cloud.

Attack Analytics – Ensures complete visibility with machine learning and domain expertise across the application security stack to reveal patterns in the noise and detect application attacks, enabling you to isolate and prevent attack campaigns.

Client-Side Protection – Gain visibility and control over third-party JavaScript code to reduce the risk of supply chain fraud, prevent data breaches, and client-side attacks.

Imperva Data Security Solutions
Imperva protects all cloud-based data stores to ensure compliance and preserve the agility and cost benefits you get from your cloud investments:

Cloud Data Security – Simplify securing your cloud databases to catch up and keep up with DevOps. Imperva's solution enables cloud-managed services users to rapidly gain visibility and control of cloud data.

Database Security – Imperva delivers analytics, protection and response across your data assets, on-premise and in the cloud – giving you the risk visibility to prevent data breaches and avoid compliance incidents. Integrate with any database to gain instant visibility, implement universal policies, and speed time to value.

Data Risk Analysis – Automate the detection of non-compliant, risky, or malicious data access behavior across all of your databases enterprise-wide to accelerate remediation.

Most small business owners surveyed report that cyberattacks have increased in recent years, and 70% say they're "highly concerned" by the situation—up 31% since 2020.

They have good reasons to be concerned about cybersecurity. The cost of data breaches for small businesses starts above $100,000, and for companies under 500 employees, it averages $3 million.

Preventing security incidents must now be a top priority for small and mid-sized businesses—beginning by learning what kinds of security incidents to guard against. This article covers the most common cybersecurity incident categories.

Learn More: Free Cybersecurity Tools For Small Business

What Is A Security Incident?
A security incident is an unauthorized attempt to access, modify, or destroy an organization's digital assets and information systems.

Security incidents can range from malware infections and phishing attempts to full-scale data breaches and ransomware attacks, with the average incident now costing small businesses well into six figures.

The key is catching these incidents early – companies typically have less than 62 minutes from first detection to prevent a security incident from becoming a major breach.

Whether it's a sophisticated cyber attack or an accidental misconfiguration by an employee, these incidents pose serious risks to business operations and data security.

What Causes Security Incidents?
The vast majority of cyber attacks are caused by some form of human error, leveraging the mistakes that people make to gain entry or bypass detection. Those mistakes include everything from recycling passwords and clicking malicious links in phishing emails to neglecting patching or over-granting privileges.

Persistent and frustrating as human errors may be, it suggests that security incidents could drop dramatically with better training and more automation.

Real World Examples Of Security Incidents
Far from a hypothetical threat, security incidents are affecting—and in some cases ending—small businesses across America:

Brilles: An online sunglasses retailer with just three employees, Brilles was targeted for a DDoS attacks that shut down their website—and sole revenue source—for months. Switching URLs promoted a repeat incident, forcing the company to close permanently.
G&J Pepsi: When this family-owned bottling plant was hit by a ransomware attack, they refused to pay, instead shutting down everything and working systematically through the incident response process. Despite recovering everything, the attack cost the G&J Pepsi around $25,000 and kept the IT team fully occupied for over six weeks.
Frank's Remedies – The solopreneur behind this skin care company clicked an innocent looking email, unaware that it was a phishing scam designed to steal his PayPal login information. Over $2,200 was drained from his account, leaving his business in a precarious financial position.

Free Incident Response Policy
Skip the policy-writing hassle with our ready-to-use incident response policy template.

Download Now

What Are The Types Of Security Incidents?

Security incidents comes in many forms, choose different targets, utilize unique tactics, and cause varying degrees of damage—and new versions emerge all the time.

Figuring out how to prevent cyber attacks must include a focus on all these common types of cybersecurity incidents:

1. Social Engineering

Social engineering coerces people to click links, extend access, or provide login credentials by manipulating their psychology. Attackers might use real names, places, dates, and other details (stolen from social media) to appear legitimate and trustworthy, among countless other ways these security incidents occur.

As many as 90% of attacks leverage some form of social engineering, simply because it's so effective. The damage can be devastating, too, since attacks can potentially bypass security controls and gain direct access to sensitive data.

Learn More: Why Is Social Engineering Effective?

Stopping social engineering takes training and awareness to prevent things like phishing attacks, combined with detection and response since these security incidents have proven notoriously difficult to avoid.

2. Ransomware / Malware

Malware inflicts damage by hiding malicious code inside software. One example is ransomware, where the code either steals or encrypts data, then hackers demand payment to restore access to the data or keep it from being released.

Malware is one of the oldest and most enduring causes of security incidents, and ransomware has been one of the most aggressive and expensive causes in recent years; ransom payments topped $1 billion in 2023, almost double the previous year.

Small businesses can protect themselves from ransomware and other malware with things like antivirus and firewall protections. They also need to understand common ways ransomware spreads through organizations and adapt security policies and training methods in response.

3. Password Attacks

Password attacks often precede information security events since passwords—and other login credentials—are the fastest and easiest way to gain unauthorized access to systems and data.

Ways to get someone's password include stealing it through phishing attacks, credential stuffing, and brute force—hackers put tremendous energy and ingenuity into this effort.

Identity attacks are some of the most devastating since they are harder to see and stop quickly—and password attacks make up 99% of the 600 million daily identity attacks logged by Microsoft.

Picking strong passwords, replacing them regularly, and enabling multi-factor authentication will all help prevent security incidents, but password discipline is difficult, so incident response must be a priority as well.

Learn More: Sample Password Policy Template

4. Credential Stuffing

Credentials stuffing happens when attackers take databases of known login credentials and use them on other sites and services, hoping to find reused credentials.

Frequent data breaches give attackers access to ever-larger amounts of compromised credentials they can weaponize, and the rise of AI makes it easier than ever to stuff credentials at scale or maximize success rates.

Identity security provider Okta reports that almost a quarter of the identity attacks it observes involve credential stuffing, and security incidents will likely climb as this tactic becomes more potent and accessible.

Devastating data breaches can result from just one bad login, making it essential to fight credential stuffing by using password managers, picking stronger authentication methods, and upgrading the speed and visibility of incident response.

Free Security Policy Templates
Get a step ahead of your cybersecurity goals with our comprehensive templates.

Download Now

5. Business Email Compromise (BEC)
Considered a subset of social engineering, attacks known as business email compromise target the inbox with messages that appear to be from superiors, collaborators, and vendors asking for money, access, or data using convincing language mixed with legitimate information.

These attacks have proven so successful that they've stolen over $50 billion over the previous decade according to the FBI.

AI that makes it easier to harvest information, imitate speaking and writing styles, or create like-like avatars will significantly increase the threat (and losses) of BEC in coming years.

Employee cybersecurity training, especially around email security, lowers the risk of BEC, however this is a sophisticated threat orchestrated by determined hackers, making it hard to stop reliably.

Be prepared to detect, contain, and eradicate what can't be prevented.

6. Supply Chain Attacks
In supply chain attacks, malicious actors gain access to a target by way of a third-party.

They will breach one company, then use the trusted relationships and integrated technology that company has with vendors, business partners, and customers to breach other companies, often without raising red flags or encountering many obstacles.

In one infamous example, hackers were able to breach the software maker SolarWinds and hide malicious code in a software update that later caused data breaches at major companies and government agencies.

By design, supply chain attacks are difficult to detect and deter, and they're on the rise, costing companies $46 billion in 2023 and projected to cost $138 billion by 2031.

7. Insider Threats
Insider threats come from employees, contractors, of vendors working "inside" the organization, where they have access and permissions that can be abused, whether accidentally or intentionally.

Compromising people, in many cases, poses fewer challenges than compromising secured systems, making insiders a popular target for attackers.

Developments like the rise of the hybrid office and the emergence of AI increase the risk of insider threats, which increased at 74% of organizations in 2023. Another contributor is increasingly complex IT environments, which are harder for users to navigate securely.

To prevent insider threats, it takes a combination of training, policies, continuous monitoring, and incident response all working in sync.

8. Web Application Attacks
When attackers find vulnerabilities or implementation issues in web applications, they can attack those applications to steal sensitive information, gain unauthorized system access, or take critical applications offline.

Incidents like these have become more damaging as companies rely on larger numbers of web applications to enable remote work.

One vendor observed more than 18 billion attacks on web application just over the course of 2023.

Web application penetration testing can reduce the risk of these attacks by exposing vulnerabilities before they get exploited, provided those vulnerabilities get remediated in time.

9. IoT Attacks
Internet-connected devices (known as IoT devices) are ubiquitous in the digital world, and they are developed and deployed so quickly that many have inadequate or minimal cybersecurity built in.

Attacks on IoT devices went up by 100% between 2021 and 2024, both because they make for easy targets and because they can be lucrative launch pads for larger attacks on sensitive information and essential IT.

From eavesdropping on video conferences to taking control of a moving car, IoT attacks can have many alarming effects, especially as they proliferate.

Learn More: How To Prevent Wireless Network Attacks

Defenses against IoT attacks include password security, network segmentation, and regular patching, but there will

always be gaps, making it important to complement prevention with detection and response.

10. Mobile Device Attacks
Mobile devices are also IoT devices, so it comes as no surprise that they share many of the same vulnerabilities for the same reasons. Mobile apps and devices have weak security while containing large amounts of sensitive information and security permissions, making them a natural target for cybersecurity attacks.

One analysis showed a 50% increase in mobile device attacks in 2023 alone, topping 33 million attacks overall.

Security teams, much like developers, still need to take threats to mobile devices more seriously, especially as things like malware and phishing attacks prioritize mobile targets.

Bring your own device (BYOD) policies, encryption, and patching play important roles in mobile security, along with an incident response plan for threats that breakthrough.

11. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
In both these types of attacks, servers are flooded with traffic until they go offline, taking critical apps, services, and data with them. Denial of services attacks send the traffic from one source while the distributed variety sends it from multiple sources.

The average DDoS attack cost $500,000 in 2023, a sharp increase caused by the duration of the average attack quadrupling in one year.

These attacks can make it impossible to conduct business, so every minute counts.

Some best practices to keep from getting overwhelmed by malicious traffic include rate limiting, network segmentation, and continuous monitoring – plus immediate response capabilities if an attack occurs.

12. Advanced Persistent Threats (APTs)
Often the most sophisticated threats in the wild, APTs infiltrate a company's IT infrastructure, then establish a long-term presence, lurking undetected while they gather intelligence and lay the groundwork for larger attacks, often leading to security incidents with deep consequences.

An APT attack on Equifax resulted in the breach of 150 million people's records and cost the company at least $425 million.

These attacks are often carried out by nation-state-sponsored cybercriminals with the best resources in the world and powerful motivations to succeed, underlining how malicious APTs can be.

Stopping them takes a cybersecurity strategy that combines offensive measures like penetration testing with defensive measures such as network monitoring and incident response.

13. Zero-Day Exploits
A zero day exploit is a vulnerability that is known by attackers but not by vendors, meaning there is no existing fix for the flaw and likely insufficient cybersecurity.

These exploits are especially dangerous because they don't set off alarm bells when compromised, nor is there an easy way to prevent the problem.

Growth in the number of cybercriminals has meant the discovery of zero-day exploits in larger quantity and less time. An annual list of the 15 most exploited vulnerabilities contained a majority of zero-days for the first time in 2023.

Since these attacks are unknown by definition, stopping them takes the combined efforts of firewalls, antivirus, intrusion protection, and security policies.

Learn More: How To Build A Cybersecurity Program

14. Man-in-the-Middle (MITM) Attacks
As the name implies, man-in-the-middle attacks position themselves between two ends of a communication channel and steal or even alter data traveling in-between.

In one simple example, attackers make malicious Wi-Fi hotspots available in a public place, wait for someone to connect, then steal data throughout their session, including login credentials.

These attacks can lead to unauthorized access to almost anything, followed by any amount of damage and disruption, making them important to address with stronger access controls around sensitive information and improved monitoring—particularly as one report showed a 35% increase in MITM attacks after 2022.

Create A Security Incident Response Plan

Preventing phishing attacks and avoiding data breaches takes many different cybersecurity measures—but perhaps none more important than an incident response plan.

Planning and preparation are essential for being able to leap into action and work effectively whenever and wherever a security incident arises.

An incident response plan outlines the roles, responsibilities, policies, and procedures to follow during a security incident to eliminate errors, inefficiency, and uncertainty.

Every business needs to create a plan for security incidents, starting by picking a security framework to follow from NIST, SANS, or another authority. Save time by following a template that specifies what exactly to include in the incident response plan.

Then create an incident response policy that aligns with your security resources and business goals. Important as it may be to implement an incident response plan, even more important is keeping it updated as staff, technology, and threats all evolve.

Learn More: 7 Proven Security Incident Response Steps For Any Breach

In today’s cyber threat landscape, effective incident management through accurate recording and reporting is crucial for mitigating damage and enhancing an organisation’s overall security posture. A well-documented and reported incident helps in understanding the root cause, evaluating the response, and preventing future occurrences. Additionally, proper reporting ensures regulatory compliance and keeps stakeholders informed, fostering trust and transparency. This blog post will walk you through the steps to accurately record a security incident, ensuring your organisation is prepared to handle cyber threats efficiently.

1. Preparation and Initial Response

Identify Key Personnel

Before an incident occurs, ensure you have a designated incident response team (IRT) in place. This team should include individuals from IT, legal, compliance, and public relations, among others. Assign roles and responsibilities clearly.

Establish an Incident Response Plan

Develop and maintain a comprehensive incident response plan (IRP) outlining procedures for identifying, responding to, and recording security incidents. Ensure this plan is accessible and regularly updated.

Incident Detection

Use automated monitoring tools and manual processes to detect potential security incidents. These tools might include intrusion detection systems (IDS), antivirus software, and security information and event management (SIEM) systems.

2. Incident Identification

Verify the Incident

Once a potential incident is detected, verify its authenticity. Analyse the initial indicators and validate them against known threats. This might involve checking logs, system alerts, and other relevant data sources.

Classify the Incident

Once detected, the incident should be classified based on its severity and type. Common categories include malware attacks, phishing attempts, data breaches, and denial-of-service attacks. Assign a severity level such as low, medium, or high to prioritise the response effort.

3. Containment

Immediate Actions

Take immediate steps to contain the incident. This could involve isolating affected systems, blocking malicious IP addresses, or disabling compromised accounts. The goal is to prevent the incident from causing further damage.

Short-Term Containment

Implement short-term containment measures to stabilise the situation. For instance, you might redirect network traffic, apply temporary fixes, or use quarantine techniques to limit the impact.

4. Eradication

Identify Root Cause

Conduct a thorough investigation to identify the root cause of the incident. This involves analysing logs, examining affected systems, and consulting threat intelligence sources.

Remove Threat

Once the root cause is identified, take steps to remove the threat completely. This could involve deleting malware, closing vulnerabilities, and applying patches. Ensure that all affected systems are clean and secure.

5. Recovery

Restore Systems

Once the threat is removed, you should begin the process of restoring systems to normal operation. This includes recovering data from backups, reinstalling software, and verifying that systems are functioning correctly.

Monitor for Further Issues

After systems are restored, continue to monitor them closely for any signs of residual issues or further attacks. Ensure that all systems are fully operational and secure.

6. Documentation and Reporting

Record Incident Details

Accurately document all details of the incident. This should include:

Date and Time: When the incident was detected, contained, eradicated, and resolved.

Description: A detailed description of the incident, including how it was detected, and the systems affected.

Actions Taken: A step-by-step account of the actions taken during the response, including containment, eradication, and recovery efforts.

Impact: An assessment of the impact on the organisation, including data loss, financial costs, and operational disruptions.

Root Cause Analysis: A detailed analysis of the root cause and any contributing factors.

Create an Incident Report

Compile the recorded details into a comprehensive incident report. This report should be clear, concise, and accessible to all relevant stakeholders. Include lessons learned and recommendations for improving incident response in the future.

Legal and Regulatory Reporting

If the incident involves data breaches or other regulatory concerns, ensure that all required legal and regulatory notifications are made promptly. This might include notifying affected individuals, regulatory bodies, and law enforcement agencies.

7. Post-Incident Review
Conduct a Post-Incident Review

A post-incident review meeting should be held with the incident response team and other relevant stakeholders. Discuss what happened, what was done well, and what could be improved.

Update Policies and Procedures

Based on the review, update your incident response plan, security policies, and procedures. Implement any necessary changes to prevent similar incidents in the future.

Training and Awareness

Provide training and awareness programmes for staff to ensure they understand the updated policies and procedures. Continuous education helps in building a security-conscious culture within the organisation.

With the MetaCompliance Incident Management Solution, we formalise and simplify the process for recording an incident whilst ensuring that all incidents and breaches are reported in a consistent fashion. Our solution removes the guesswork for your employees by providing concise, guided questions to capture key information.

Conclusion
Recording and reporting a security incident accurately is a vital component of an effective incident response strategy. By following these steps, organisations can ensure they are well-prepared to handle incidents, minimise damage, and improve their overall security posture. Proper reporting not only helps in regulatory compliance but also fosters trust among stakeholders by maintaining transparency.

Remember, the goal is not just to respond to incidents but to learn from them and enhance your defences continually. With a comprehensive approach to incident management, your organisation can stay resilient in the face of evolving cyber threats.

10 types of security incidents and how to prevent them

Cyberattacks are more varied and numerous than ever. Learn the key signs of common security incidents and how to respond to keep systems and data safe.
By
TechTarget ContributorAlissa Irei, Senior Site Editor
Published: 12 Jan 2024
Security incidents are events that put the confidentiality, integrity or availability of an organization's systems or data at risk. A security incident may or may not result in compromised data, depending on whether measures in place to protect the digital environment succeed or fail.

In IT, a security event is anything that has significance for system hardware or software, and an incident is an event that disrupts normal operations. Security events are usually distinguished from security incidents by the degree of severity and the associated potential risk to the organization.

If just one user is denied access to a requested service, for example, that may be a high-severity security event because it could indicate a compromised system. On the other hand, the access failure could be due to any number of relatively innocuous factors. Typically, that one event doesn't have a severe impact on the organization and, therefore, doesn't qualify as an incident.

If large numbers of users are denied access, however, it likely means there's a more serious problem, such as a DoS attack. In that case, the event is classified as a security incident.

This article is part of

What is incident response? A complete guide
Which also includes:
10 types of security incidents and how to prevent them
The 9 best incident response metrics and how to use them
Top incident response tools: How to choose and use them
A security breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed or disclosed in an unauthorized fashion.

Unlike a security breach, a security incident doesn't necessarily mean information has been compromised -- only that

the information was threatened. For example, an organization that successfully thwarts a cyberattack has experienced a security incident but not a breach.

How to detect security incidents

Nearly every day brings a new headline about one high-profile data breach or another. But many more incidents go unnoticed because organizations don't know how to detect them.

Here are some signs enterprises can look for to uncover security incidents:

Unusual behavior from privileged user accounts. Any anomalies in the behavior of a privileged user account can indicate someone is using it to gain a foothold in a company's network.
Unauthorized insiders trying to access servers and data. Many insiders test the waters to determine exactly what resources they can access. Warning signs include unauthorized users attempting to access servers and data, requesting access to data that isn't related to their jobs, logging in at abnormal times from unusual locations or logging in from multiple locations in a short time frame.
Anomalies in outbound network traffic. It's not just traffic that comes into a network that organizations should worry about. Organizations should monitor for traffic leaving their systems as well. This could include insiders uploading large files to personal cloud applications; downloading large files to external storage devices, such as USB flash drives; or sending large numbers of email messages with attachments outside the company.
Traffic sent to or from unknown locations. For a company that only operates in one country, any traffic sent to other countries could indicate malicious activity. Administrators should investigate any traffic to unknown networks to ensure it's legitimate.
Excessive consumption. An increase in the performance of server memory or hard drives may mean an attacker is accessing them illegally.
Changes in configuration. Changes that haven't been approved, including reconfiguration of services, installation of startup programs or firewall changes, are a sign of possible malicious activity. The same is true of scheduled tasks that have been added.
Hidden files. These can be considered suspicious because of their file names, sizes or locations, which indicate the data or logs may have been leaked.
Unexpected changes. These include user account lockouts, password changes or sudden changes in group memberships.
Abnormal browsing behavior. This could be unexpected redirects, changes in the browser configuration or repeated pop-ups.
Suspicious registry entries. This happens mostly when malware infects Windows systems. It's one of the main ways malware ensures it remains in an infected system.

Common attack vectors

An attack vector is a path or means by which a hacker can gain access to a computer or network server to deliver a payload or malicious outcome. Attack vectors enable malicious hackers to exploit system vulnerabilities, including end users.

Attack vectors include viruses, email attachments, webpages, pop-up windows, instant messages, chatrooms and deception. All these methods involve software or, in a few cases, hardware. The exception is deception, which is when a human end user is fooled into removing or weakening system defenses.

Although organizations should be able to handle any incident, they should focus on those that use common attack vectors. These include the following:

External/removable media. The attack is executed from removable media -- e.g., CD, flash drive or peripheral device.
Attrition. This type of attack uses brute-force methods to compromise, degrade or destroy networks, systems or services.
Web. The attack is executed from a website or web-based application.
Email. The attack is executed via an email message or attachment. A hacker entices the recipient to either click on a link that takes them to an infected website or to open an infected attachment.
Improper usage. This type of incident stems from the violation of an organization's acceptable use policies by an authorized user.
Drive-by downloads. A user views a website that triggers a malware download; this can happen without the user's knowledge. Drive-by downloads, which take advantage of vulnerabilities in web browsers, inject malicious code using JavaScript and other browsing features.
Ad-based malware (malvertising). The attack is executed via malware embedded in advertisements on websites. Merely viewing a malicious ad could inject malicious code into an insecure device. In addition, malicious ads can also be embedded directly into otherwise trusted apps and served via them.
Mouse hovering. This takes advantage of vulnerabilities in well-known software, such as PowerPoint. When a user hovers over a link -- rather than clicking on it -- to see where it goes, shell scripts can be launched automatically. Mouse hovering takes advantage of system flaws that make it possible to launch programs based on

innocent user actions.
Scareware. This manipulates users into purchasing and downloading unnecessary, unwanted and potentially dangerous software. Scareware tricks user into thinking their computers have viruses and then recommends that they download and pay for fake antivirus software to correct the problem. If a user downloads the software and allows the program to execute, however, malware may infect the system.
Understanding attackers' methodologies and goals
Although an organization can never be sure which path an attacker will take through its network, hackers typically employ a certain methodology -- i.e., a sequence of stages to infiltrate a network and steal data. Each stage indicates a certain goal along the attacker's path. This security industry-accepted methodology, dubbed the Cyber Kill Chain, was developed by Lockheed Martin Corp.

According to Lockheed Martin, these are the stages of an attack:

Reconnaissance -- i.e., identify the targets. Threat actors assess potential targets from outside the organization to identify the ones that best enable them to meet their objectives.

The goal of attackers is to find information systems with few protections or with vulnerabilities they can exploit to access the target system.
Weaponization -- i.e., prepare the operation. During this stage, attackers create malware designed specifically to exploit the vulnerabilities discovered during the reconnaissance phase. Based on the intelligence gathered in that phase, attackers customize their tool sets to meet the specific requirements of the target network.
Delivery -- i.e., launch the operation. The attackers send the malware to the target by any intrusion method, such as a phishing email, a man-in-the-middle attack or a watering-hole attack.
Exploitation -- i.e., gain access to victim. The threat actors exploit a vulnerability to gain access to the target's network.
Installation -- i.e., establish beachhead at the victim. Once malicious hackers have infiltrated the network, they install a persistent backdoor or implant to maintain access for an extended period of time.
Command and control -- i.e., remotely control the implants. The malware opens a command channel, enabling the attackers to remotely manipulate the target's systems and devices through the network. The malicious hackers can then take control of all affected systems from its administrator.
Actions on objectives -- i.e., achieve the mission's goals. What happens next, now that attackers have command and control of the target's system, is entirely up to them. They may corrupt or steal data, destroy systems or demand ransom payments, among other things.
The Cyber Kill Chain model identifies the seven steps that advanced persistent threats follow: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.
The Cyber Kill Chain helps cyber defenders anticipate adversaries' actions.
10 common types of security incidents and how to prevent them
Many types of cybersecurity attacks and incidents could result in intrusions on an organization's network. These include the following.

1. Unauthorized attempt to access systems or data
To prevent a threat actor from gaining access to systems or data using an authorized user's account, implement MFA. This requires a user to provide a password, plus at least one additional piece of identifying information.

Additionally, encrypt sensitive corporate data at rest and as it travels over a network, using suitable software or hardware technology. That way, attackers aren't able to access confidential information.

2. Privilege escalation attack
An attacker who gains unauthorized access to an organization's network may then try to obtain higher-level privileges using what's known as a privilege escalation exploit. Successful privilege escalation attacks grant threat actors privileges that normal users don't have.

Typically, privilege escalation occurs when the threat actor takes advantage of a bug, misconfiguration, programming error or any vulnerability in an application or system to gain elevated access to protected data.

This usually occurs after a malicious hacker has already compromised a network by gaining access to a low-level user account and looks to gain higher-level privileges -- i.e., full access to an enterprise's IT system -- either to study the system further or perform an attack.

To decrease the risk of privilege escalation, organizations should look for and remediate security weak spots in their IT environments on a regular basis. They should also follow the principle of least privilege – i.e., limit the access rights for users to the bare-minimum permissions they need to do their jobs -- and implement security monitoring.

Organizations should also evaluate the risks to their sensitive data and take the necessary steps to secure that data.

3. Insider threat
This is a malicious or accidental threat to an organization's security or data typically attributed to employees;

former employees; or third parties, including contractors, temporary workers or customers.

To detect and prevent insider threats, implement spyware scanning programs, antivirus programs, firewalls, and a rigorous data backup and archiving routine. In addition, train employees and contractors on security awareness before allowing them to access the corporate network. Implement employee monitoring software to reduce the risk of data breaches and the theft of intellectual property by identifying careless, disgruntled or malicious insiders.

4. Phishing attack
In a phishing attack, a threat actor masquerades as a reputable entity or person in an email or other communication channel. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including extracting login credentials or account information from victims. A more targeted type of phishing attack known as spear phishing occurs when the attacker invests time researching the victim to pull off an even more successful attack.

Effective defense against phishing attacks starts with educating users to identify phishing messages. In addition, a gateway email filter can trap many mass-targeted phishing emails and reduce the number of phishing emails that reach users' inboxes.

5. Malware attack
This is a broad term for different types of malware that are installed on an enterprise's system. Malware includes Trojans, worms, ransomware, adware, spyware and various types of viruses. Some malware is inadvertently installed when an employee clicks on an ad, visits an infected website, or installs freeware or other software.

Signs of malware include unusual system activity, such as a sudden loss of disk space; unusually slow speeds; repeated crashes or freezes; an increase in unwanted internet activity; and pop-up advertisements. Installing an antivirus tool can detect and remove malware. These tools can either provide real-time protection or detect and remove malware by executing routine system scans.

6. DoS attack
A threat actor launches a denial-of-service (DoS) attack to shut down an individual machine or an entire network so that it's unable to respond to service requests. DoS attacks do this by flooding the target with traffic or sending it some information that triggers a crash.

An organization can typically deal with a DoS attack that crashes a server by simply rebooting the system. In addition, reconfiguring firewalls, routers and servers can block any bogus traffic. Keep routers and firewalls updated with the latest security patches.

Also, application front-end hardware that's integrated into the network can help analyze and screen data packets -- i.e., classify data as priority, regular or dangerous -- as they enter the system. The hardware can also help block threatening data.

7. Man-in-the-middle attack
A man-in-the-middle (MitM) attack is one in which the attacker secretly intercepts and alters messages between two parties who believe they are communicating directly with each other. In this attack, the attacker manipulates both victims to gain access to data. Examples of MitM attacks include session hijacking, email hijacking and Wi-Fi eavesdropping.

Although it's difficult to detect MitM attacks, there are ways to prevent them. One way is to implement an encryption protocol, such as TLS, that provides authentication, privacy and data integrity between two communicating computer applications. Another encryption protocol is SSH, a network protocol that gives users, particularly system administrators, a secure way to access a computer over an insecure network.

Enterprises should also educate employees to the dangers of using open public Wi-Fi, as it's easier for hackers to hack these connections. Organizations should also tell their workers to pay attention to warnings from browsers that sites or connections may not be legitimate. Companies should also use VPNs to help ensure secure connections.

8. Password attack
This type of attack is aimed specifically at obtaining a user's password or an account's password. To do this, malicious hackers use a variety of methods, including password-cracking programs, dictionary attacks, password sniffers and guessing passwords via brute force -- i.e., trial and error.

A password cracker is an application program used to identify an unknown or forgotten password for a computer or network resources. This helps an attacker obtain unauthorized access to resources. A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password.

To prevent password attacks, organizations should adopt MFA for user validation. In addition, users should choose strong passwords that include at least seven characters, as well as a mix of upper and lowercase letters, numbers and symbols. Users should change their passwords regularly and use different passwords for different accounts. In

addition, organizations should use encryption on any passwords stored in secure repositories.

9. Web application attack
This is any incident in which a web application is the vector of the attack, including exploits of code-level vulnerabilities in the application, as well as thwarting authentication mechanisms. One example of a web application attack is a cross-site scripting attack. This is a type of injection security attack in which an attacker injects data, such as a malicious script, into content from otherwise trusted websites.

Enterprises should review code early in the development phase to detect vulnerabilities; static and dynamic code scanners can automatically check for these. Also, implement bot detection functionality to prevent bots from accessing application data. Finally, a web application firewall (WAF) can monitor a network and block potential attacks.

10. Advanced persistent threat
An advanced persistent threat (APT) is a prolonged and targeted cyberattack typically executed by sophisticated cybercriminals or nation-states. In this attack, the intruder gains access to a network and remains undetected for an extended period of time. The APT's goal is usually to monitor network activity and steal data rather than cause damage to the network or organization.

Monitoring incoming and outgoing traffic can help organizations prevent hackers from installing backdoors and extracting sensitive data. Enterprises should also install WAFs at the edge of their networks to filter traffic coming into their web application servers. This can help filter out application layer attacks, such as SQL injection attacks, often used during the APT infiltration phase. Additionally, a network firewall can monitor internal traffic.

Examples of security incidents
Here are several examples of well-known security incidents:

Cybersecurity researchers first detected the Stuxnet worm, used to attack Iran's nuclear program, in 2010. It is still considered one of the most sophisticated pieces of malware ever detected. The malware targeted SCADA systems and spread through infected USB devices. Both the U.S. and Israel have been linked to the development of Stuxnet, and while neither nation has officially acknowledged its role in developing it, there have been unofficial confirmations that they were responsible for it.
In October 2016, another major security incident occurred when cybercriminals launched a DDoS attack on domain name system provider Dyn, which disrupted online services worldwide. The attack hit a number of websites, including Netflix, Twitter, PayPal, Pinterest and PlayStation Network.
In July 2017, a massive breach was discovered involving 14 million Verizon Communications Inc. customer records, including phone numbers and account PINs, which were reportedly exposed to the internet, although Verizon claimed no data was stolen. A month earlier, a researcher from security firm UpGuard found the data on a cloud server maintained by data analytics firm Nice Systems. The data wasn't password-protected, and as such, cybercriminals could have easily downloaded and exploited it, according to the security firm.
In 2023, casino giant Caesars Entertainment fell victim to a social engineering campaign that led to the exposure of sensitive customer data, including Social Security numbers. Threat actors reportedly called the IT service desk and tricked personnel into resetting MFA factors for Okta super administrator accounts. MGM suffered a similar incident the same month, resulting in an estimated $100 million in losses.
Trends in the causes of incidents
According to the 2023 "Data Security Incident Response Report" by U.S. law firm BakerHostetler, the number of security incidents and their severity remain high. Even as organizations implement new security measures, attackers find ways to circumvent them.

In analysis of more than 1,160 incidents, BakerHostetler found network intrusions were most common, accounting for nearly half of all security incidents. Thirty percent of incidents were business email compromise attacks, and 12% involved inadvertent disclosure of private information.

The most common known root cause was phishing, which kicked off one in four security incidents. Unpatched vulnerabilities were behind 11% of cases; social engineering and other human error each drove 5% of incidents.

Ransomware was involved in 28% of incidents analyzed. Across all industries, the average time to recover after a ransomware attack increased over the previous year, as did the average ransom payment.

On the bright side, detection and response capabilities improved. The median number of days to detect an attack was three -- down from 13 the previous year. The median time from discovery to containment took zero days. The time from containment to forensic analysis also decreased from 30 to 24.

Create an incident response plan
The expanding threat landscape puts organizations at more risk of being attacked than ever before. As a result, enterprises must constantly monitor the threat landscape and be ready to respond to security incidents, data breaches and cyberthreats when they occur.

Putting well-defined incident response plans in place enables organizations to effectively identify these incidents, minimize the damage and reduce the costs of cyberattacks. Such plans also help companies prevent future attacks.

Editor's note: This article was originally written in 2019. TechTarget editors revised it to improve the reader experience.

Alissa Irei is senior site editor of TechTarget Security.