ON THE DEFENSE

Data breaches can cause devastating financial losses. According to the report, the biggest contributor to these costs is detection and escalation. Detection and escalation involve activities related to detecting breaches, such as security audits and forensic investigations. The second biggest contributor is lost business. This consequence can linger for years because of the reputational harm that an organization experiences. Regulatory fines can also impact an organization. Organizations that host the data of European Union (EU) residents or do business with EU countries face some of the stiffest penalties per the General Data Protection Regulation (GDPR), an extensive data privacy law and regulation.

The rising cost of breaches is a key driver for the cybersecurity industry. And the number of high-profile cases will probably increase as more countries adopt data standards such as those in the GDPR.

53% of reporting companies suffered a cyberattack, up 48% from the previous year. The median spent on cybersecurity was USD 155,000, a 39% increase over three years. The median cost for attacks decreased slightly from around USD 16,000 to 17,000. As businesses have spent more money on their cybersecurity measures, the cost of attacks has decreased. One out of eight attacks cost more than USD 250,000. Small businesses, defined as those with under ten employees, spent four times more on cybersecurity than they did two years prior. Still, the number of small businesses that experienced an attack increased from 23% to 36% over three years. One out of three companies experienced consequences from payment diversion fraud, the leading cause of financial loss for businesses. Payment diversion fraud is where an attacker tricks an organization into rerouting payments intended for suppliers or other business expenses into a bank account that the attacker controls. One out of five companies received a ransom demand. The percentage of companies paying the ransom dropped from 66% to 63%. The reason for this shift might be better awareness of how to deal with ransomware attacks and that paying ransoms isn’t always the best decision.

Regardless of the reasons for the decrease, organizations should continue seeking professional guidance when they experience ransomware attacks. Experts can recommend strategies for recovering data, negotiating with attackers, handling legal consequences, and preventing future attacks.

These statistics show that cyberattacks are an unavoidable cost of doing business. Organizations must increase their cyber resilience and implement effective security strategies. A good metaphor for a cyberattack is that of a pollutant in the environment. The accumulation of attacks is something that everyone must deal with. Organizations cannot ignore the attacks forever, and doing so only exacerbates the problem.

A security strategy is an organization’s well-defined plan to protect its digital and physical assets. A comprehensive security strategy consists of the following components. Risk assessment helps to identify and understand potential threats and vulnerabilities that can impact assets. Security policies and procedures establish rules for maintaining security. Security awareness and training provide employees with the knowledge and skills to prevent security breaches. Incident response (IR) comprises the set of actions that an organization takes to prepare for, detect, stop, and recover from cyberattacks. Auditing and testing ensure that security measures are effective and work as intended.

An IT security team or a specialized cybersecurity consultant is usually responsible for creating an organization’s security strategy. Ideally, this strategy should be in place as soon as an organization forms, but it’s never too late to start, and the sooner, the better! The organization should review and update its security strategy annually, if not more frequently, to ensure that it remains effective and relevant given emerging threats and the organization’s changing objectives and technologies.

An organization’s security strategy is vital to its overall security maturity. Security maturity is how well an organization can protect its assets and respond to cybersecurity threats. The more advanced and well-defined an organization’s security protocols and strategies, the greater its maturity level.

Organizations have many security maturity models to choose from when evaluating their maturity. For simplicity’s sake, we’ll focus on one popular model: the Cybersecurity Capability Maturity Model (C2M2). Developed collaboratively by private and public sector organizations, C2M2 is designed to help organizations assess the state of their cybersecurity capabilities. Organizations can use it as a guide to progress from a less mature state, where cybersecurity measures might be reactive or poorly developed, to a more mature state, where measures are proactive, optimized, and well-integrated into the organizational culture.

C2M2 uses a scale with four maturity indicator levels (MILs): MIL0, MIL1, MIL2, and MIL3. The levels differ by specific behaviors, practices, and processes relating to cybersecurity. The following table summarizes the characteristics of each maturity indicator level.

|  |  |
| --- | --- |
| ***Level*** | ***Characteristics*** |
| ***MIL0*** | Practices are not performed |
| ***MIL1*** | Initial practices are performed but might be ad hoc |
| ***MIL2*** | Management characteristics:   * Practices are documented * Adequate resources are provided to support the process   Approach characteristic:  Practices are more complete or advanced than at MIL1 |
| ***MIL3*** | Management characteristics:   * Activities are guided by policies or other organizational directives * Responsibility, accountability, and authority for performing the practices are assigned * Personnel performing the practices have adequate skills and knowledge * The effectiveness of activities is evaluated and tracked   Approach characteristic:  Practices are more complete or advanced than at MIL2 |

To understand how organizations can apply C2M2, consider the following example from the US Department of Energy. The example shows the model used to evaluate an organization’s ability to reduce vulnerabilities.

At MIL1, one or more organization members perform the following actions to reduce vulnerabilities: Identifies data sources ad hoc to support vulnerability discovery, Collects and analyzes vulnerability data ad hoc, Performs vulnerability assessments ad hoc, Mitigates relevant vulnerabilities ad hoc.

At MIL2, one or more organization members perform the following actions to reduce vulnerabilities: Monitors vulnerability data sources that address higher-priority assets, Performs vulnerability assessments regularly and when key events occur, such as changes to the network, Analyzes identified vulnerabilities, ranks them by severity, and then addresses them appropriately, Evaluates operational impact before applying mitigations such as patches, Shares information about vulnerabilities with stakeholders.

At MIL3, one or more organization members perform the following actions to reduce vulnerabilities: Monitors vulnerability data sources that address all relevant IT and OT assets, Ensures that people independent of the operations being assessed perform vulnerability assessments, Reviews the effectiveness of vulnerability mitigation, Establishes and maintains ways to receive and respond to external reports, such as from public websites, about vulnerabilities relevant to the organization’s IT and OT assets.

To develop their security strategy, organizations must first decide where to start. What type of cybersecurity do they need, and where should they focus their resources, such as employees, capital, and time? The National Cyber Security Centre’s 10 Steps to Cyber Security are:

Risk management: Take a risk-based approach to securing your data and systems. Engagement and training: Collaboratively build security that works for people in your organization. Asset management: Know what data and systems you have and what business need they support. Architecture and configuration: Design, build, maintain, and manage systems securely. Vulnerability management: Keep your systems protected throughout their lifecycle. Identity and access management: Control who and what can access your systems and data. Data security: Protect data where it is vulnerable. Logging and monitoring: Design your systems to be able to detect and investigate incidents. Incident management: Plan your response to cyber incidents in advance. Supply chain security: Collaborate with your suppliers and partners.

When organizations develop a security strategy, they rarely need to start from scratch or work in isolation to achieve their objectives. A vast marketplace of security products and services exists. Most large organizations have products from various cybersecurity vendors. For example, they might use one vendor’s data loss prevention system (DLP) and another vendor’s firewall. These varied companies contribute to a vibrant ecosystem supported by standard authorities, charities, and government entities.

A perfect, unbeatable security strategy doesn’t exist. Attackers always develop new techniques to bypass security measures, making current defenses obsolete. A more realistic and effective security strategy focuses on making successful attacks more difficult to achieve. By doing so, organizations can deter all but the most determined attackers. Imagine that compromising a certain organization’s system would cost an attacker USD 100,000 worth of resources. If the compromised system is worth only USD 80,000 to the attacker, then the attacker is unlikely to attack. Therefore, the defense can work despite its imperfections.

A practical yet effective security strategy often involves layering defences, updating and patching systems regularly, and investing in threat intelligence to stay ahead of emerging threats. These measures increase the time, cost, and effort required to complete a successful attack, in turn dramatically reducing the likelihood of a breach.

The goal of cybersecurity is to reduce operational risk to an acceptable level by introducing the correct mixture of education, processes, and technologies. Some strategies that organizations use to prevent cyberattacks: Reduce the attack surface, Create a demilitarized zone (DMZ), Follow the principle of least privilege, Manage software vulnerabilities, Use defence in depth.

One of the first concepts to consider is attack surface. An attack surface is all the points in a system where an attacker can attempt to enter it, impact it, or obtain data. The attack surface includes all points of vulnerability, such as interfaces, protocols, and services. The larger the attack surface, the greater the risk of infiltration. Therefore, a primary goal of any good security strategy is to keep the attack surface as small as possible. Doing so minimizes vulnerabilities, making the system less attractive and more difficult for attackers to breach.

Consider an organization that has a payment record system. To reduce the system’s attack surface, the organization restricts employees’ system access to several office locations. As a result, its cybersecurity team can ignore external internet traffic at the perimeter, significantly reducing the attack surface for potential attackers. Instead of having countless IP addresses from which to launch an attack, attackers must first compromise a trusted device, and then use it for further attacks. This added layer of complexity increases the challenge for attackers.

Organizations keep giving employees more ways to access internal systems. For example, many organizations provide remote access methods and permit employees to access systems from personal devices. These features have helped to improve accessibility, service offerings, and employment flexibility. But they’ve also expanded the attack surface. As a result, establishing a secure perimeter has become more challenging. Organizations must be aware of their perimeter and proactively monitor it.

A vital part of secure system design is a demilitarized zone. A demilitarized zone (DMZ) is a network segment between an organization’s internal, private network and the internet. It’s a buffer zone that adds an extra layer of safety. To access the internal network, attackers must go through the DMZ. Even if they breach the DMZ, the internal network is still safe.

Typically, DMZs house servers that must be accessible from the wider internet yet still need protection. These servers might include web, email, file transfer protocol (FTP), and DNS servers. These servers contain public data, not sensitive internal data.

A legitimate external user can access servers and applications contained in the DMZ, the segment between the external and internal firewalls. But this user cannot access more sensitive servers and applications in the internal network behind the internal firewall. For example, a customer might be able to place orders for a digital payment system or access email. Still, they cannot access employee records or other customers’ financial data on the internal network.

Organizations must decide the appropriate levels of permission for applications and employees. They should do so following the principle of least privilege: grant a user or application the fewest permissions needed to complete their function.

An organization sets up its human resources (HR) database so that managers have read-only access to data for the job roles that they manage. If an attacker steals a certain manager’s credentials, then the attacker can only compromise the confidentiality of those specific records. The attacker cannot modify them because they are read-only. Also, the attacker cannot access applications for other areas of the business.

By introducing this control, the organization reduces the consequences of a successful attack compared to one on a less restricted system. And by reducing the consequences, the organization reduces the risk value. You might see the military term blast radius applied in this context, in which the radius indicates an attack’s area of effect. Reducing permissions is an effective way to limit the blast radius.

Software vulnerability management involves monitoring and mitigating vulnerabilities in software systems. It includes patch management, the process of applying patches and updating systems as fixes become available.

When a vendor creates a new version of its software, it might decide to stop supporting the older version. For example, Microsoft no longer supports older versions of Windows, such as Windows 7. As a result, the company no longer releases security patches, making Windows 7 devices easy targets for attackers. When possible, organizations should use software versions that the vendor supports. Otherwise, they should implement compensating controls that reduce the risk associated with known vulnerabilities. These controls might include disabling certain features, increasing network security, or increasing monitoring to detect suspicious activity.

Generally, updating software and applications to their latest versions significantly reduces the risk of a successful attack. Still, new versions of software can also introduce vulnerabilities. Organizations must check with vendors to know what and when patches are available. If a vendor has no fix for a vulnerability, organizations can implement temporary compensating controls, such as disabling a feature or reverting to a previous version.

An organization can use a vulnerability scanner to assess what software is vulnerable to a specific attack. A vulnerability scanner is an application that scans a system for known vulnerabilities, such as outdated software, missing patches, misconfigured settings, or weak passwords. Some vulnerability scanners are network-based, examining vulnerabilities by active testing. Others scan static source code for possible errors. Both scanners produce valuable information for identifying flaws before an attacker does.

Another key consideration for defense is for organizations to use a layered approach. The term defense in depth derives from the military; instead of relying on a single form of defense, you layer them. The meaning is similar in IT. Defense in depth is a strategy in which you use multiple layers of controls to protect assets. Perimeter -> Network -> Host -> Application -> Data.

For example, an organization might apply the following layers of security: network defenses such as firewalls, device defenses such as malware scanners, data defenses such as encryption. For an attack to succeed, it must compromise or circumvent all these layers, which is challenging.

A standard method for attacking a system is malware and a standard measure for detecting malware is antimalware software. Antimalware software, or antivirus software, is specialized software that detects, quarantines, and even destroys malware on computers or networks. Some well-known antimalware programs include Malwarebytes, McAfee Antivirus, and Windows Defender Antivirus. You can install this software locally on a single device or run and manage the software on a centralized server.

Antimalware software detects malware by scanning all device files for signatures. A malware signature is a pattern of attributes that corresponds to known malware. After identifying a signature in a file, the software deletes the file, quarantines it, or alerts you that the file might be infected.

One of the most essential methods for attack detection is logging. Logging is the process where actions are accurately recorded in a secure location. Log records should be tamper-proof and act as a permanent record of what has occurred within a network. You can perform logging on individual machines or applications.

The types of actions logged depend on the organization’s systems and security needs. Commonly logged actions include user logins and logouts, failed login attempts, system configuration changes, packet traffic, and process or service initiation. Also, logs often record alterations to files or databases.

Though a single log entry might not be highly valuable in isolation, a larger collection helps track activities of legitimate users and malicious actors. These logs provide an audit trail invaluable for diagnosing issues and identifying malicious activity or security breaches.

The following log entry shows the log format that Apache web servers use: 9.12.156.2 - bob [11/Jan/2020:14:16:34 -0700] “GET /index.html HTTP/1.0” 200 4066

Notice that this log entry describes a user named bob who is accessing a specific web page with the status and time noted.

In addition to recording events happening on servers, organizations can monitor communications across their network. This approach, known as traffic analysis, can identify network activity, even encrypted activity. Traffic analysis involves tracking different metrics related to the network. Some examples of these metrics include the source and destination of traffic, network protocols used, bandwidth used, and packet size. Advanced traffic analysis can also identify specific applications or services in use, the presence of any malicious code, and unusual behavior or anomalies that might indicate a cyberattack. Some types of malware pivot from device to device in ways that good network monitoring tools can easily identify.

Imagine a network monitoring tool is in use. If someone uses a network device to stream video, then the tool will show high bandwidth consumption from the device over an extended period. Conversely, if someone uses a network device to download a large file, then the tool will show a high demand peak for the device and then little or nothing after that point.

Making sense of all the data collected through network monitoring can be challenging. For help, many cybersecurity professionals turn to security information and event management (SIEM) tools. A security information and event management (SIEM) tool collects all the data throughout an organization’s technology infrastructures and aggregates it so the cybersecurity team can identify and analyze events and patterns of potential attacks.

Imagine that a cybersecurity team suspects that an attacker is trying to compromise a user’s account using brute force attacks. They can use a SIEM tool to detect brute force login attempts for that account. To do so, they might set an alert to trigger if five or more failed logins occur per minute for the account. Suppose an attacker attempts to compromise the account by working through millions of username or password combinations. In that case, the attacker will exceed the threshold, triggering the alert in the SIEM tool and notifying the team.

The group responsible for looking after an organization’s security is often part of the security operations center. A security operations center (SOC) is a dedicated team of cybersecurity professionals that uses specialized software to actively monitor, detect, investigate, and respond to an organization’s potential security threats and incidents in real time. One of the SOC’s key objectives is to detect attacks in progress using SIEM and other monitoring tools.

Security analysts in a SOC are responsible for assessing an organization’s security. If they detect an attack or potential attack, they will decide how to respond to it following organizational procedures.

False alarms: One challenge in SOCs is determining the best thresholds for alerts. Their goal is to reduce false positives, which are legitimate events incorrectly recorded as malicious. Confirming if an alert is a false positive is the responsibility of a security analyst. If a specific legitimate event triggers too many false positives, the analyst should consider setting the thresholds higher.

Consider an employee who returns to work after a long holiday and forgets her password. If she guesses her password incorrectly, then her repeated attempts might exceed the threshold, triggering an alert.

Artificial intelligence (AI) is enhancing organizations’ attack detection and defense. Let’s explore how AI impacts key areas of attack detection.

Logging: AI automates the process of logging and analyzing large volumes of data from various sources. This manual task would take a human an enormous amount of time, but AI can do it very quickly, enabling real-time threat detection and prevention.

Network monitoring: AI can analyze traffic patterns and identify anomalies that might indicate an attack. For example, a sudden surge in network traffic might indicate a distributed denial-of-service (DDoS) attack. With AI, organizations can detect such anomalies instantly and initiate appropriate countermeasures.

SIEM tools: SIEM tools use AI to collate and analyze data across an organization’s network. These tools identify patterns and correlations, helping to identify potential security threats. For example, QRadar SIEM sets alert thresholds for abnormal activities, such as multiple failed login attempts.

SOCs: Organizations can train AI systems to distinguish between normal and unusual behavior. The AI trains on historical data that includes legitimate threats and false positives. With the help of machine learning algorithms, the AI system learns to recognize patterns associated with false positives. For example, the system might determine that a certain number of failed login attempts from a trusted internal IP address during working hours is a common pattern of a forgotten password, not a malicious action. Therefore, the system learns not to trigger an alert in this situation. Over time, it can become better at reducing false positives, thereby fine-tuning the thresholds and alert sensitivity. It can even reduce the time spent on false positives by automating the verification process.

The SANS Institute provides many educational courses, events, and online resources relating to cybersecurity, including an industry-standard framework for incident response. Let’s briefly review the six phases of this framework.

Phase 1: Preparation: An organization starts planning what it will do when an incident occurs. Typical steps include preparing resources and testing procedures.

Phase 2: Identification: The security team detects the security event. Then, the team initiates the incident response protocol to investigate further and confirms that the event is an actual security incident, not a false alarm.

Phase 3: Containment: The security team works to prevent the situation from worsening. Typical steps include segregating networks and shutting down access routes or certain systems.

Phase 4: Eradication: The security team works to completely remove the presence and impact of the malware or attackers. For example, the team might wipe devices or restore them to safe states. Incomplete eradication often results in malware re-emerging, so eradication efforts must be thorough.

Phase 5: Recovery: The organization returns to standard operation. Typical steps include removing temporary fixes and restoring certain services.

Phase 6: Reflection: The security team and relevant parties reflect on the incident’s cause and the response’s effectiveness. Some incident response frameworks referred to this phase as the lessons learned phase. However, the lessons identified phase might be a better title if the organization makes no changes!

This incident response framework provides a solid baseline to build upon. Some types of attacks or incidents require expanding certain stages. For example, consider a data breach event from a lost storage device. The eradication phase might be short and simple, but the recovery phase might be longer with more stakeholders engaged.

As part of standard business activities, many organizations will go through several simulated activities to test their level of preparation: paper-based tests, tabletop exercises, and live tests.

In a paper-based test, security teams complete surveys about their level of preparation. They might have to identify key personnel, explain how to create proper backups, and explain how to produce process documents upon request.

A tabletop test is a more involved test format. In this test, key personnel come together to simulate the incident response process end-to-end. A benefit of this test is that teams can interact with one another and see how the broader scenario would develop.

Live tests, or tests in the live systems, are the most realistic form of testing. Organizations can shut down critical systems to test various failures and how their teams respond.

Business continuity refers to an organization’s ability to continue operating despite an incident. For example, an organization might have backup sites to take over the delivery of services or a backup technology to take over should one fail. Disaster recovery refers to an organization’s ability to recover from a disaster. For example, imagine that an incident disaster wipes all an organization’s computers or deletes entire databases. In this recovery planning process, organizations must be prepared to start with virtually nothing.

Continuity planning and disaster recovery have high levels of overlap with other security functions. Concerns used to mainly pertain to natural disasters such as floods, earthquakes, or fire. Now, cyberattacks can be equally or more disruptive than their natural counterparts. For example, a power cut is extremely unlikely to hit all of a multinational organization’s sites simultaneously; however, a cyberattack that shuts down key global services, such as organizational file shares or domain management systems, is far more plausible.

Organizations benefit from having incident response teams. Response plans can save money. For example, consider the findings in the Cost of a Data Breach Report 2023(opens in a new tab). At organizations with incident response capabilities, the average cost of a breach was USD 3.62 million in 2023. At organizations without incident response capabilities, the average cost of a breach was USD 5.11 million. This average cost was a difference of USD 1.49 million, or 34%.

Cryptography is the principles, means, and methods of transforming data to conceal its content, prevent its unauthorized use, or prevent its undetected modification. One key objective of cybersecurity is keeping data confidential. Keeping and sharing secrets has been challenging for thousands of years. Though methods for preserving confidentiality have changed significantly across the years, the objective has remained broadly the same.

Secure, reliable communications have three properties: confidentiality, authenticity, and integrity. Cybersecurity professionals commonly use three fictional characters: Alice, Bob, and Eve. Alice and Bob want to communicate securely, but Eve wants to eavesdrop on the exchange. Confidentiality: Alice can send a message to Bob without Eve being able to understand the contents. The message remains private. Authenticity: Eve cannot send a message to Bob claiming to be Alice. Authenticity includes ensuring that spoofing or impersonation is impossible. Integrity: If Eve modifies a message between Alice and Bob, then the receiver can detect that the message has been modified. Note that you can tamper with messages without knowing the contents. For example, people can talk loudly to disrupt a face-to-face conversation in a language they do not understand.

A standard method for preserving a message’s confidentiality is encryption. Encryption is the process of converting a message into something understandable only to those with a decryption key to reverse the process. A message converted into an unreadable state is encrypted.

When you encrypt data, you use a cipher. A cipher is a set of transformations that converts plaintext, the intelligible, human-readable data, into ciphertext, the data’s encrypted form. To convert plaintext, the cipher follows a key, which is a blueprint for which transformations to make.

At a high level, modern-day encryption comes in two forms: symmetric and asymmetric.

In symmetric encryption, the algorithm for encrypting information uses the same key as the decryption process. Symmetric encryption is fast and easy to implement. It relies on both the sender and receiver having access to the same key, similar to a password or shared secret, to maintain a private information link.

A simple example is a rotation-based cipher in which characters are increased or decreased by a fixed number of places in the alphabet. The number of places to move forward and backward acts as the key. If the sender uses a key of +1, they rotate characters forwards by 1, and then the receiver uses a -1 rotation to receive the original message. In the following cipher, the word HOLIDAY is encrypted by a +1 shift in the alphabet to be IPMJEBZ.

The Advanced Encryption Standard (AES) is a commonly used algorithm for symmetric encryption. It uses a secret key to transform plaintext into ciphertext. Only those with the correct key can decrypt the ciphertext. Organizations use AES to protect sensitive data such as passwords and financial transactions.

In asymmetric encryption, also known as public key encryption, you use one key to encrypt data and a different key to decrypt it. These keys are known as public keys and private keys, and you generate them simultaneously. You can share your public key with others. Anyone with a copy of this key can use it to encrypt a message before sending it to you. But decrypting that message requires using your private key, which you should keep secret.

In the following diagram, Alice is the sender, and Bob is the receiver. It represents the transmission process. Alice encrypts a message by using Bob’s public key. Once the message is encrypted, it can only be decrypted using Bob’s private key. Alice sends the encrypted message to Bob. Bob decrypts the message by using his private key. Finally, Bob can read the message. Bob must not share his private key with anyone. Otherwise, they would be able to read all his incoming messages.

The main benefit of asymmetric encryption is that organizations can communicate securely with an entity with which they have not previously exchanged a key. In addition, this type of encryption helps ensure that a message goes to the correct receiver.

One benefit of asymmetric cryptography comes from online shopping. You can buy goods from shops without physically going to the location to create a shared, unique, symmetric key. If symmetric cryptography were the only option, the agreed symmetric key would be required to encrypt and decrypt all future transactions between you and the shop. In contrast, using asymmetric cryptography is convenient and saves time because you don’t need to meet in person. Without this benefit, secure online shopping is practically impossible.

Quantum computing is a rapidly emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers. So, how does quantum computing relate to cryptography? It’s a threat in the hands of cyberattackers. Its ability to factorize large prime numbers, the base for existing cryptography, might render current encryption methods ineffective. Organizations need new strategies to defend against this new threat. Enter quantum-safe encryption.

Quantum-safe encryption refers to security methods and protocols resistant to quantum computing attacks. Experts have proposed many post-quantum cryptography alternatives to defend against quantum computing attacks. Let’s explore the four types of encryption that experts predict will effectively counter quantum computing attacks:

Lattice-based encryption uses multidimensional geometric structures to encrypt data, creating a puzzle that is challenging for even quantum computers to solve. Hash-based encryption transforms data into a character string by using a hash function. The result is a unique output that is difficult to reverse engineer, even for quantum computers. Multivariate encryption uses several different math equations and variables at the same time. This approach is highly complex and tough for quantum computers to crack. Code-based encryption transforms data into encoded messages that are difficult to decode without the correct algorithm, even for quantum computers.

Cyberthreat intelligence, or simply threat intelligence, is data that an organization has collected and analyzed to understand the motives and behavior of threat actors. Intelligence typically focuses on attacker tactics, techniques, and procedures (TTPs) or other indicators of compromise (IoCs).

Tactics are the why, meaning the adversary’s tactical goal or reason for performing an action. For example, an adversary might want to increase privileges. Techniques are the how, meaning the ways that an adversary achieves a tactical goal by performing an action. For example, an adversary might bypass access controls to increase privileges. Procedures are the specific implementation that the adversary uses for techniques. For example, an adversary might use a specific tool or program to increase privileges. Indicators of compromise (IoCs) are signatures related to attacker activity. For example, some IP addresses might be associated with threat actor groups or certain files. An IoC’s presence can indicate that an organization has already been compromised, hence the name.

Organizations can benefit from threat intelligence across the following broad areas. Providing a warning: A key benefit of threat intelligence is it helps organizations prepare for attacks. Certain geopolitical or technical developments can rapidly change an organization’s risk profile. But with advance notice, organizations can better prepare their defenses to prevent an attack from occurring at all. Providing indicators of compromise (IoCs): Threat intelligence aids detection activities by providing IoCs. Some examples of these IoCs include IP addresses, file hashes, or domains associated with attackers. An organization’s security analyst can search for these signs and add detection rules that trigger an alert when they are detected. Providing context: When attacked from an unknown location or group, an organization can use intelligence sources to start understanding the attacker. Context can include helpful pieces of information to aid attribution and guidance on what to expect next. Learning from peers: Organizations can share information about how attackers attacked them, how they defended themselves, and how effective their approaches were. Sharing these stories helps strengthen the whole industry.

Gathering and developing threat intelligence can be complex. Organizations can directly collect information themselves or use information from other sources. Let’s examine some common threat intelligence sources that organizations use.

Threat exchange platforms: Cybersecurity professionals can use various online platforms to access databases of gathered information and analysis. Some of these platforms are freely accessible to anyone, although others are available only to subscribers or closed industry groups. One example of an industry-standard threat exchange platform is IBM X-Force Exchange.

Conferences: Cybersecurity professionals can share the latest industry developments at conferences. To get more publicity at a conference, some researchers hold off revealing their discoveries to the public. Conferences also provide opportunities to gather information through informal conversations and to network. Examples of relevant conferences include Black Hat, RSA Conference, and CYBERUK.

Articles and news: Some media outlets, such as Security Intelligence, devote significant coverage to developments in the IT world. And as some security issues gain a higher profile, the coverage has increased significantly. Many smaller sites and traditional media outlets cater to cybersecurity specialists. Examples of cybersecurity blogs include Krebs on Security and Graham Cluley.

Product videos: Organizations such as Microsoft, Google, and Apple, which produce a lot of software, release periodic security advisories relating to their products. These advisories can include critical security information and are essential reading for system administrators.

Computer systems can gather and process data much faster than humans, making artificial intelligence (AI) especially valuable for obtaining threat intelligence. Let’s explore several types of AI-enabled threat intelligence.

Natural language processing (NLP): AI-enabled natural language processing (NLP) systems can automatically recognize and pull out key data points about threats. Notably, NLP systems extract these points from unstructured data. That’s data, such as images and text messages, that lacks any built-in structure that typical computers can easily read. Conventional data tools and methods struggle to process and analyze it. But NLP systems can effectively parse unstructured data sources, such as social media feeds and news articles, to collect relevant threat intelligence. The technology helps organizations stay current on IoCs and attack methods.

Threat intelligence sharing: Combating emerging threats isn’t an individual effort; it requires organizations and security teams to share threat intelligence. Traditional sharing methods involve manual, often time-consuming processes. But with AI, organizations can automate sharing. Plus, the technology is sophisticated enough to share information pertinent to the threat without disclosing personally identifiable information, strategic plans, or other confidential data.

Predictive analytics: AI is especially useful for predictive analytics. Predictive analytics is a type of analytics where you combine historical data with techniques such as statistical modeling and machine learning to make predictions. With AI, organizations can create more effective predictive models, helping them anticipate and address threats before they arise.

With threat intelligence, organizations can act in a systematic and planned way rather than using estimations or relying on standards. The result is defenses designed to meet the attacks that they will experience rather than defenses designed only to meet an industry or regulatory standard. This distinction is particularly important for organizations that operate in a complex or anomalous way, for which regulations often provide insufficient guidance.

The biggest contributor to the cost of a data breach is detection and escalation, followed by lost business. A comprehensive security strategy includes risk assessment, policies and procedures, awareness and training, incident response, and auditing and testing. The more advanced an organization’s security protocols and strategies, the greater its security maturity. Common strategies for preventing attacks include reducing the attack surface, following the principle of least privilege, managing software vulnerabilities, and using defense in depth. Standard methods for detecting attacks include antimalware software, logging, network monitoring, security information and event management (SIEM) tools, and security operations centers (SOCs). Artificial intelligence (AI) can enhance an organization’s attack detection in many ways, such as by reducing false positives. The SANS Institute’s incident response framework includes six phases: preparation, identification, containment, eradication, recovery, and reflection. Secure, reliable communications have three properties: confidentiality, authenticity, and integrity. In symmetric encryption, you use the same key to encrypt and decrypt data. In asymmetric encryption, you use a public key to encrypt data and a private key to decrypt it. Organizations will need quantum-safe encryption methods to defend against quantum computing attacks. Threat intelligence provides many benefits, such as warning about emerging threats and identifying indicators of compromise (IoCs). Common sources of threat intelligence include media outlets and threat exchange platforms, such as IBM X-Force Exchange.