

Cyber Chief

Magazine

Ed.15

Understanding Insider
Threats

Just-in-Time Administration
for Secure Access
Management



**Staying Cybersafe:
Practical Steps for
Organizations**

Cyber Chief

Magazine

This edition of Cyber Chief Magazine celebrates National Cybersecurity Awareness Month! It comes packed with the resources that organizations need to secure their data and defend against cyberattacks.

This year, a month dedicated to cybersecurity awareness feels more relevant than ever. Organizations around the world are seeking ways to ensure security for their remote and hybrid workforces as cybercrime becomes ever more pervasive and damaging. To protect their critical data and systems, IT pros need to continually seek out accurate information and implement proven best practices.

Cyber Chief Magazine is here to help. The October edition offers both broad strategies and specific tactics that empower organizations to take proactive steps to enhance cybersecurity. Use these articles to reflect on your organization's security journey and consider how to further secure the systems and information that your company depends upon.

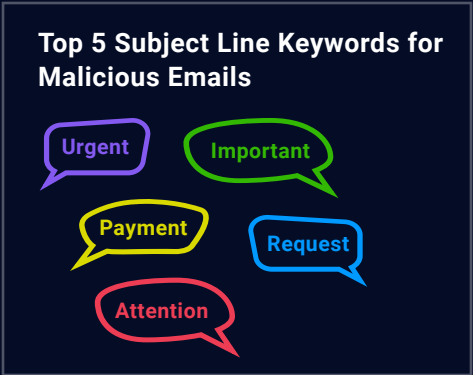


The Cyber Chief team
cyber.chief@netwrix.com

Contents

Cybersecurity: Facts and Figures

- 4 Cybersecurity awareness statistics



Focus

- 6 Just-in-Time Administration for secure access management

Analysis

- 12 How businesses can protect sensitive data against phishing attacks
- 16 Understanding insider threats

Extra Security

- 22 Five things systems leadership can do to protect data in salesforce
- 28 Cybersecurity Maturity Model Certification (CMMC): Tips for compliance
- 36 NIST cybersecurity framework: Benefits and key components
- 42 Top tactics for preventing data leaks

First-Hand Experience

- 47 Regional council eliminates security blind spots and reduces the likelihood of a breach

Cybersecurity: Why is It Important?



5.2 billion internet users which is 63% of world population



In **2020**, the number of cybercrime incidents exceeded **29,000 cases worldwide**



The global average cost per data breach was **3.86 million U.S. dollars**

Statista

IT Security Key Weak Spots



Too much data



Lack of IT security personnel



Lack of security knowledge among employees



No integration between security solutions

Ransomware

IN 2021

ransomware criminals REvil demanded \$50 million from Acer

In 2021 a company is affected by ransomware

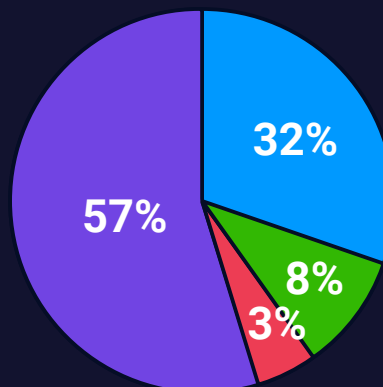
EVERY 11 SECONDS

\$220,298

is the average ransom demand in 2021

Ransomware Attack Vectors shift as New Software Vulnerability Exploits Abound (coveware.com)

How Companies Recover after Ransomware



Backup recovery

Other recovery

Paid ransom

Didn't recover

Types of Cybercrime



Malware

- Ransomware
- Viruses
- Worms
- Spyware



Bots

- DoS (denial of service)
- DDoS (distributed denial of service)
- Credential theft



Social engineering

- Phishing
- Baiting
- Swatting



Physical cyberattacks

- USB driver with virus
- Attacker pretends to be an employee
- Identity theft

Phishing

43% of breaches involved phishing or pretexting, making it the most frequent cybercrime

The number of phishing incidents in 2020 was **241,324**

96% of phishing attacks were pulled off by using email scams

Top 5 Subject Line Keywords for Malicious Emails



Tessian

Verizon

The Symantec ISTR 2019

Focus

Just-in-Time Administration for Secure Access Management

Martin Cannard

VP of Product Strategy at Stealthbits - Now part of Netwrix



Although external cybersecurity attacks and malware make for sensational headlines, the biggest security threat most organizations face comes from trusted insiders with privileged access to sensitive data. Cybersecurity Insider's [2020 Insider Threat Report](#) reveals that 68% of organizations report that insider attacks are becoming more frequent and that they feel vulnerable to them.

The security challenge of standing privileges

One of the basic principles of data security is providing least privileged access, which reduces your risk surface by only allowing specific privileges for specific purposes. However, this principle is easily violated by standing privileges — account privileges that are always available, even when not needed — which provide a perpetually available attack surface.

Use of accounts with standing privileges is very common; in particular, many organizations issue privileged accounts to all administrators in the mistaken belief that they need unrestricted access to effectively do their jobs. These accounts often include access to more systems than necessary and are always available for use, which violates the principle of least privilege.

As long as the accounts — and, by extension, the privileges — exist, the security risk remains.

What are just-in-time permissions?

A just-in-time (JIT) permissions model reduces the privilege attack surface to only the times when privileges are actively being used, as opposed to the 24/7 attack surface of always-on privileges.

When a user needs to complete an activity that requires elevated permissions, they complete a request describing what the task is and the resources they need to do it. If the request is approved, they are provisioned with a temporary identity with just enough privilege (JEP) to complete the task. Once the task is completed, the identity is disabled or deleted.

However, it's important to know that not all JIT access solutions actually reduce the attack surface area. Some vendors create accounts that are provided to users upon request, but the accounts remain active after use, with all of their permissions intact, instead of being disabled or deleted. This is often true of privileged access management (PAM) tools and password vaults. As long as privileged accounts exist, all of the risks of standing privileges remain in your system.

Why are just-in-time permissions important for your organization?

Securely implemented JIT permissions offer multiple benefits:

- **Stronger cybersecurity.** JIT permissions significantly reduce the risk of access credentials being stolen by attackers and used to access sensitive data or move laterally through your IT ecosystem. It also reduces the risk of credential misuse, either malicious or negligent, by account owners.
- **Simplified administration.** Implementing JIT privileged account management empowers admins to access the resources they need quickly while eliminating all the management tasks associated with standing accounts, such as frequent password changes.
- **Compliance.** Implementing the least privilege principle and establishing control over privileged accounts are requirements of all major compliance regulations. Auditors pay special attention to these areas, and gaps can lead to steep fines. Eliminating standing privileged accounts helps you avoid audit findings.

Approaches to just-in-time administration permissions

There are several different approaches to JIT permissions. Look for the one that best balances your organization's security, risk, and operational objectives, and also consider the effort it will take to change your current procedures.

- **Temporary elevation.** A user's own account is granted extra permissions for a limited amount of time. When the time is up, the additional access is revoked
- **Broker and remove access.** One or more standing privileged accounts are created and their credentials are stored in a central vault. Users must provide a justification when requesting to use one of the accounts to access specific systems for a specific amount of time.
- **Zero standing privilege (ZSP).** There are no standing privileged accounts. Instead, temporary privileged accounts are enabled or created based on specific needs and destroyed or disabled after use. Privileged access must be requested for the time required to complete a particular task that requires elevated permissions for a specific system, database, or application. If the request is approved, access

is granted. Once the task is completed, the access is revoked.

Benefits of Zero Trust framework

As part of your organization's ongoing risk management and data security strategy, you should work toward a goal of zero standing privileges. Eliminating "always-on" privileged access in favor of JIT permissions help ensure that systems and data are accessible only when there is a valid reason to do so.

A quality ZSP solution can help your company implement multiple Zero Trust best practices, including the following:

- **Segregation of duties:** No user or device should have full access to all IT sources.
- **Least privileged access:** Users and devices can access only the resources they need.
- **Micro-segmentation:** The IT environment should be split into different security zones that require separate authorization.
- **Just in time access:** Users and devices gain elevated access only when required and only for as long as required.
- **Auditing and tracking:** A log is maintained of every request for elevated access, whether that access was granted, and when it was revoked.

How Netwrix can help

Netwrix SbPAM eliminates standing privilege. It creates just-in-time accounts with just enough privilege to complete the task at hand and then removes them. As a result, there are no user accounts with privilege for hackers to compromise or for account owners to accidentally or deliberately misuse.

[Netwrix SbPAM](#) can help your organization:

- **Reduce privileged access security risks.** You can eliminate standing privileges altogether. Alternatively, you can choose to elevate user access permissions for an existing account just enough to perform a required task and revoke those additional rights automatically afterward.
- **Regain control over privileged accounts.** Know exactly who has access to critical systems, reduce elevated access to the absolute minimum, and maintain a least-

privilege access state to keep identity security risks low.

- **Enhance admin accountability.** See exactly what privileged activity is happening across your systems with live or retrospective session monitoring.
- **Minimize your attack surface with the automatic cleanup.** Mitigate the risk of pass-the-hash, Golden Ticket, and related attacks with automatic purging of Kerberos tickets after each privileged session.
- **Protect your service accounts by rotating their passwords from one place.** Receive an alert if the process is disrupted so you can pause the process and roll back any unwanted changes.

GUIDE

Privileged Access Management Best Practices

[Learn More](#)

How Businesses Can Protect Sensitive Data Against Phishing Attacks

Ilia Sotnikov

VP of User Experience & Security Strategist

In the recent [Verizon Data Breach Investigations Report](#), phishing was one of the top listed threat actions that led to actual data breaches, alongside stolen credentials and user errors. As the threat of phishing has increased tremendously during the pandemic, it's not surprising that we have seen an increase in coverage about data breaches that began with phishing attacks. One of the most recent examples was the [SANS Institute](#) – the firm that, ironically, offers cybersecurity training. This breach compromised 28,000 records, exposing potential hackers and cyber-criminals to sensitive personal data such as email addresses, work titles, first name, last name, work phone, company name, industry, address, and country of residence. This threat requires organisations not only enhance data security, but also improve their capabilities to detect incidents and recover from them.

Why are phishing attacks so common?

In spite of continuous efforts of IT teams to mitigate the risk of phishing, these efforts have frequently proven to be unreliable. The reason for this is a piecemeal approach to cybersecurity that is still the case for the majority of organisations, especially SMBs. For example, if an organisation has properly set up its spam filters and updated its anti-malware solutions but failed to enhance its detection capabilities, it might fail to detect an ongoing

attack. All in all, it is inevitable that the anti-phishing strategy requires from an organisation a thorough approach. Without such a holistic approach to cybersecurity, threat actors will prevail. As law-abiding organisations, we have to be vigilant 100% of the time. The bad guys need only one point of entry to be successful in their nefarious pursuits.

TIP 1.

Keep spam filters tuned and up to date

One of the common mistakes that many organisations make is to leave their spam filters with the default settings. While this is definitely better than not having any spam filters at all, this approach will lead to large number of false positives. While the majority of service providers do update their filters based on threat intelligence, simply relying on this is not enough. There will always be attacks specific to an organisation's industry or geography, or just targeted at the certain company. As no service provider can effectively account for all of this, it makes sense for organisations to tweak their filters based on what the employees actually receive.

TIP 2.

Invest in training

While efficient spam filters do protect an organisation from emails that are being

distributed from suspicious domains, they will not identify a malicious email sent from a legitimate domain. This includes, a compromised supplier's domain, or, worse yet, a compromised corporate account. With this type of phishing, employees truly are the first line of defence. Organisations should regularly conduct phishing awareness training sessions, which might range from virtually free tools such as a newsletter from the IT Security Team to advanced training programmes.

Employees should be trained to identify unusual requests such as attackers' attempts to lure the employee into sharing or uploading data or transferring funds. They should be aware of basic principles of identifying a phishing email such as hovering over links to check out where they lead or checking the information independently from the contacts inside the email, etc. People should know how to verify unusual and urgent requests and how to react on them. It is also important that employees report such emails to the IT team, especially, the ones that are sent from corporate accounts.

TIP 3.

Keep your anti-malware technologies up to date

Even if people are cyber security trained, they are prone to errors. Up-to-date endpoint protection and anti-malware are critically important to

back up and prevent the negative impact when users fall prey and open a malicious attachment or follow a link to malware-infecting website. Regular patching saves an organisation from threats that might come with phishing emails, and from the threat of hackers exploiting vulnerabilities that might occur in any software.

TIP 4.

Make anti-phishing strategy part of overall security strategy

Though all the above measures help organisations minimise the risk of hackers breaking into their networks and stealing sensitive data, they do not completely eliminate this risk. To avoid a patchwork approach to anti-phishing policy and data security, IT leaders must think bigger and employ additional security controls to minimise the possible damage. This includes limiting access to sensitive data, regularly revoking excessive privileges to decrease the attack surface, enabling auditing to speed up mean-time-to-detect and reacting to security incidents faster. An inevitable aspect of such a strategy is gaining visibility into what types of sensitive data an organisation has and where it resides. By knowing this, organisations will be able to detect files outside of their secure locations and eliminate sensitive data overexposure.

GUIDE

How to Prevent Ransomware Infections: Best Practices

[Learn More](#)

Analysis

Understanding Insider Threats

Elena Vodopyan

Manager of Content Marketing

Insider threats remain one of the biggest issues plaguing cybersecurity. [A study by Ponemon](#) shows that the costs of insider threats leaped 31% in just two years, from \$8.76 million in 2018 to \$11.45 million in 2020. The same report shows that it takes companies an average of 77 days to contain an insider threat incident. [Forrester predicts](#) that insider threats will cause 31% of data breaches by the end of 2021, up from 25% in 2020.

Both government and businesses are certainly aware of the issue, but the resources required to address it often outpace the IT security budgets. [Insider threat prevention](#) needs to consider lots of things: corporate infrastructure and technologies used, data stored, data sensitivity levels, data protection measures, data security and privacy mandates, and local cultural norms and labor practices.

In this article, we will look at the problem carefully, starting with the types of insider threats and then discussing how security threat actors operate and how to identify and mitigate the risk.

What is the insider threat?

The insider threat is a security risk that comes from any individual with legitimate access

to the organization's information and assets. That includes anyone working or connected to a company, such as current and former employees, contractors, business associates and vendors.

Types of Insider Threats

There are three types of insider threats: insiders who are negligent or careless; insiders with malicious intent; and hackers who become insiders by stealing legitimate system credentials.

Unintentional

Regular users and admins can both unintentionally perform actions that put the organization at risk, such as:

- Failing to protect their credentials
- Falling victim to common attacks like phishing or social engineering
- Falling behind on security patches and updates
- Sharing confidential information due to ignorance or disregard of data sensitivity levels
- Failing to follow security policies because they overcomplicate their jobs.

Intentional

Malicious insiders can purposefully take actions that benefit them but cause harm to the organization. Motivations for attacks include:

- **Espionage** — A current or former employee might use their access to a company's systems or data to gain information, such as intellectual property or proprietary data/information, with a goal to achieve a competitive advantage.
- **Revenge** — A former worker or another individual holding a grudge against an organization could use their access rights to damage the company or its people, for example, by attacking important systems or stealing and publishing executives' emails or other sensitive information.
- **Profit** — A malicious insider could use their access to make money, for example, by diverting funds from a company's account or selling sensitive data.

Compromised credentials

Another type of malicious insider threat is a hacker who steals valid user or admin credentials to get into the corporate IT network. Credential theft costs companies \$2.79 million per year, making it the most expensive form of insider threat.

Hackers use different methods to steal credentials, including:

- **Phishing emails** — Individuals inside an organization receive emails disguised as legitimate business requests, often asking for information like bank routing numbers or requesting that the recipient clicks on a link to download an attachment or visit a website.
- **Pass the hash** — This hacking technique allows an attacker to authenticate to a remote server or service by stealing the hash of a user's password instead of the plaintext password.
- **Cracking passwords** — Hackers use a variety of approaches to guess a user's password:
 - **Brute-force attacks** — Hackers run a program that attempts to log on using common passwords and working through every possible character combination.
 - **Dictionary attacks** — This tactic involves working through different phrases and word strings instead of individual characters.
 - **Spraying attacks** — Hackers use a few common passwords to attack thousands of accounts at once.
 - **Reverse brute-force attacks** — The attackers use one password to go after multiple user accounts.

Indicators of Insider Threat

What do you need to watch for to detect an insider threat? Here are some common indicators:

- Failed or successful access to systems or data outside of working hours or without a business need
- Attempts to download or copy large amounts of data
- Use of unauthorized systems, devices and software, such as public cloud storage.
- Attempts to bypass security protocols
- Corporate policy violations

The consequences of insider threat incidents

Insider threats can cause severe and costly damage to an organization. Among the consequences are:

- **Critical data loss or theft.** Insiders can accidentally or deliberately destroy intellectual property, trade secrets, personal data, customer data and other critical information, wiping out years of work in an instant.

- **Negative impact on organizational productivity**, such as delays in vital business functions like production, operations, customer service responses, and supply chain management.
- **Financial impact**, including costs related to incident investigation and the remediation of systems and processes.
- **Legal/regulatory impact**, including fines and litigation defense costs tied to complaints from individuals and organizations affected by data breaches. For example, if a healthcare organization suffers a breach of personal health information (PHI), the affected patients are at risk of identity theft and other consequences, and the organization can be slapped with penalties by regulatory bodies.
- **Loss of competitive edge.** For example, a pharmaceutical company could lose years of research into a promising drug, costing them millions in potential revenue.
- **Damage to reputation.** It can take a long time to regain the trust of customers and shareholders.

Tips to protect your organization against an insider threat

The best security technology on the market isn't enough to stop every insider attack. Organizations need a comprehensive security strategy in place that accounts for the potential of inside threats.

A good strategy requires a team effort and a willingness to refine business processes, even if it means changing company culture. Insider threat protection requires a nuanced approach. Here are the essential steps to take:

1. Classify your data according to its value and sensitivity.

It's essential to understand which information has the most value, where it's stored, and how it's accessed and used. [Data discovery and classification solutions](#) can help your company find sensitive and regulated information, classify its sensitivity level, and analyze how the data gets used.

2. Monitor user activity across the entire network.

It's important to understand exactly who is accessing what data and what they are doing with it. Focus on monitoring critical systems and data first, and then expand the scope as necessary. Choose a monitoring tool that doesn't just provide raw user activity events but that uses user

behavior analytics to identify suspicious or risky.

3. Minimize access rights and keep business accounts and personal accounts separate.

Ensure that people have access to sensitive data only as necessary for their job function. Have administrators use regular user accounts for routine business functions, and [grant them temporary elevated privileges as needed](#) to complete specific tasks. Eliminating permanent admin accounts reduces the insider threat significantly.

In addition, implement security measures like these:

- Establishing policies that prohibit password sharing
- Removing access to resources promptly when users change roles or leave the company
- Placing controls around third-party access
- Requiring multi-factor authentication for access to critical systems and data
- Regularly looking for and deleting unused accounts

4. Maintain company-wide awareness of insider threats.

Have HR teams conduct risk assessments of individuals working with privileged information. All users should regularly receive comprehensive security

training about what data access and distribution activity is and isn't allowed.

5. Automate response activities. To minimize the damage an insider can do, set up automated response actions, such as temporary blocking access to data and disabling credentials that might have been compromised.

- Detect attempts to escalate permissions
- Investigate incidents efficiently and quickly find the best response to each attack

How the Netwrix Data Security Platform can help

The Netwrix Data Security Platform simplifies [insider threat detection](#), investigation and response. With the solution, you can:

- Reduce the damage an insider could do, accidentally or deliberately, by monitoring user access rights and identifying overexposed data
- Automatically classify the data you store so you can implement appropriate controls for different types of data
- Continuously monitor the activity of regular and privileged users, and get alerts about anomalous behavior

Extra Security

Five Things Systems Leadership Can Do to Protect Data in Salesforce

Amy Carlson

Director of Customer Success at Strongpoint
now part of Netwrix

Salesforce is quickly becoming the CRM of choice for businesses of all sizes, across all industries. In Q4 of 2020, it captured an [estimated 19.8% of the CRM market share](#), more than its four closest competitors combined.

Not only are more organizations using the platform, they're using it for more things, too. Solutions like Revenue Cloud and Health Cloud, as well as a robust ecosystem of third-party apps, have expanded its scope beyond that of a conventional CRM.

Here's the bad news: the platform's widespread use among major companies means there's a strong incentive for bad actors to target personal and protected data housed on the platform. Fines, reputational damage, costly audits and even legal action are all potential consequences of not taking data security in Salesforce seriously.

So, How Secure Is Salesforce Anyway?

Like all cloud software, Salesforce offloads a lot of the work around security and compliance to the provider. However, Salesforce is also highly customizable, and that customizability creates risk. The more complex your Salesforce

environment is, the less reliable the top-down, one-size-fits-all protections put in place by the Salesforce SecOps will be.

Risk in a customized environment is complicated. A managed bundle or third-party app may push code into your system without proper review. A consultant may build an integration with outside software that creates an unexpected vulnerability. A user accessing the system incorrectly — whether deliberately or because they've been assigned the wrong permissions — may be able to create, read, edit or even delete data they shouldn't have access to.

So how can Systems and IT leadership running Salesforce be more proactive about security, while still maintaining the flexibility to change things as business requires? Here's the good news: there are a number of low-cost, low-effort things teams can start doing today that will immediately make Salesforce more secure.

Run a Security Health Check

One of your best tools for improving your Salesforce security posture is likely in your Org already — the Security Health Check. Salesforce's Security Health Check lets your team establish a security baseline — using either Salesforce's

recommended best practices or custom settings specific to your organization — and measure your performance against them.

The Health Check covers a variety of settings — session settings, password policies, certificate and key management, and more — that can be easily adjusted by your team. So while this is a bit of a cheat in terms of our list — unless your Org is in excellent shape already, a Health Check will likely create several tasks for your Admin team — it can be highly useful for level-setting when it comes to Salesforce security.

Turn on Multi-Factor Authentication

Even the most sophisticated security system can be circumvented with a stolen username and password. Whether or not you run a full Salesforce Health Check, start by implementing multi-factor authentication for all possible roles and systems. Salesforce will require MFA from internal users (ie, everyone except customers and community users) by February 2022; begin the process now — either using Salesforce’s MFA tool or via a Single Sign-On provider — and your Org will be instantly more secure, at no additional cost and very little outlay of your IT resources.

Review Access Approvals

Multi-factor authentication provides a great stepping stone to a broader review of your access policies. Think: how do you onboard and offboard employees? Who reviews and approves role assignments when an employee’s responsibilities change? Formal policies for these scenarios can be as simple as requiring an email alert to a senior manager before approval is granted. But taking a minute to spell them out — and getting buy-in from your Admin team — is a key step in improving your overall security posture.

Implement Change Controls

As we mentioned above, how your Salesforce Org is customized is a critical, and complex, risk vector. Between outside consultants, managed bundles and development activity by users, it’s one that is evolving constantly, too. Even something that seems simple, like a picklist change made by one of your admins, can affect data used in financial reporting in unpredictable ways if its impact isn’t properly reviewed and understood.

If you run a ticketing system like Jira or ServiceNow, you’ve already got some accountability built into your processes. But ticketing systems can’t account for changes

that don't follow those processes. They also don't demonstrate that what was reviewed and approved externally was what happened in your production or sandbox Org.

Build tighter change controls by scheduling regular reviews of the Salesforce audit log, or — better yet — use a tool that will automatically reconcile approvals to deployed changes (skip ahead to the end of the article if you'd like to see our recommendation).

Review Data Classification

The big stumbling block with change control (especially when you do it manually) is that, in all but the simplest cases, there aren't enough resources to review and reconcile every single change in a busy Salesforce environment. The answer? Prioritize security resources and budgets based on risk. Understanding where risk lies and how data should be protected will significantly reduce the expense and cost of implementing appropriate controls.

As the name implies, data classification is simply the process of identifying data that needs additional protection, whether due to sensitivity or regulatory scope. Since 2019, Salesforce has supported data classification for all standard

and custom object fields. This makes it possible to record, report on and track data owner, field usage, data sensitivity and compliance categorizations via metadata fields.

Going through and entering this information for every standard and custom field may seem like a lot of work, but it's work that will save time in the long run, as you'll be able to easily identify where your most sensitive data resides. From there, access controls can be more precisely targeted, and privileged data can receive the additional protection it requires.

A Last Word on Data Security in Salesforce

Data security is both a sprint and a marathon. There are quick and easy things you can do today to protect your most sensitive information, but they need to be part of a longer term, more holistic approach to systems, people and processes. Salesforce leadership can and should start with the tips in this article — and build on that foundation to implement a more effective risk management framework that meets their unique security and compliance goals.

Strongpoint, now part of Netwrix, simplifies and streamlines some of the most resource-intensive aspects of data security in Salesforce. This includes tracking and reconciling changes to in-scope access, metadata and configuration data — essentially automating what would otherwise be time-consuming manual control. The result is that teams running Strongpoint can implement extremely tight, verifiable controls that lock down sensitive and privileged data in Salesforce, without breaking the bank, and without tying up key members of their IT and Systems teams. Head over to www.strongpoint.io for more information.

EBOOK

The Salesforce Data Security Checklist

[Learn More](#)

Extra Security

Cybersecurity Maturity Model Certification (CMMC): Tips for Compliance Security

Mike Tierney

VP of Customer Success,
Security and Compliance Expert

Following a string of [83 data breaches in 2019](#) alone, the United States Department of Defense (DoD) established the Cybersecurity Maturity Model Certification (CMMC). The CMMC framework is a unified national standard for improving cybersecurity. Companies in the defense industrial base (DIB) must implement CMMC requirements in order to win contracts. Read on to find out how you can achieve compliance.

Introduction to the CMMC

CMMC is a cybersecurity standard created by the Office of the Under Secretary of Defense (OUSD) for Acquisition & Sustainment. It seeks to respond to cyber threats by standardizing the way that DoD contractors secure critical information.

To achieve CMMC certification, DIB companies must implement appropriate cybersecurity practices and processes to protect all sensitive Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) they process or store. Organizations receive a cybersecurity maturity score on a scale from one to five. This score determines the level of trust the DOD places in the organization and impacts everything from hiring to contracts.

Under previous guidelines (the Defense Federal Acquisition Regulation Supplement [DFARS] 252.204-7012), to demonstrate their cybersecurity resilience, contractors could self-attest to compliance with NIST SP 800-171. However, this model resulted in a number of high profile data breaches such as the [Solar Winds affair](#), as well as violations of the False Claims Act.

To improve cybersecurity, the CMMC now requires a CMMC third-party assessor organization to certify that contractors have met the cybersecurity requirements. The DoD plans implementation of the new CMMC requirements through a phased rollout with the additional requirements becoming effective in 2025, as discussed in more detail below.

To achieve compliance with CMMC requirements, organizations still need a thorough understanding of NIST SP 800-171, since the CMMC certification process uses that framework as guidelines to help measure system security, assess the maturity of

Who must comply with the CMMC?

The CMMC maturity model applies to every company within the DoD supply chain, including

not just those in the defense industrial base, but also those in procurement, construction or development. This includes prime contractors who interact directly with the DoD, as well as subcontractors who work with contractors to execute DoD contracts.

Size and relationship to a contract do not matter. There is no loophole for small businesses working on “minor” portions of a contract. Therefore, every contractor and subcontractor dealing with any form of defense information must prepare for a review of their cybersecurity practices. Failing to comply will not lead to monetary penalties, but being certified is a prerequisite to winning contracts.

What types of data does CMMC protect?

The CMMC protects two types of data:

Controlled Unclassified Information (CUI) —

This includes any unclassified information made by the government that needs protection. It includes private federal employee information, contractor information, legal material, technical drawings, electronic files and more. To deal with CUI, an organization must have a maturity level rating of 3 or higher.

Federal Contract Information (FCI) — FCI consists of any information that the government provides or creates under a contract in order to deliver a service or product, but that is not released to the public. Improper disclosure of this data may pose a significant threat to the inner workings of DOD logistics and activities.

Dealing with FCI requires only level 1 or 2 certifications.

CMMC timeline

Contractors have until 2025 to prepare their systems to handle FCI and CUI as required by CMMC. However, the Pentagon recently moved from deploying CMMC only in tabletop exercises to its use in the field through the [award of 15 “pathfinder” contracts](#). This pilot program focuses on level 3 companies and their subcontractors; more companies must comply as the rollout proceeds.

What is the assessment methodology?

In 2020, the DoD issued an Interim Rule that supplements the CMMC program with an assessment methodology for evaluating

whether companies are compliant. Under this rule, CMMC certification proceeds in two steps. You must repeat the certification process every three years.

Step 1. Assessors apply the [NIST SP 800-171 DoD Assessment Methodology](#) to the company. This methodology classifies potential threats to a project into three tiers (high, medium and low), based on the sensitivity of the information and programs involved. Every contractor seeking high or medium level approval must provide access to facilities, systems, and personnel. Gaining access to CUI or FCI is impossible without such scrutiny.

Step 2. If a company passes step 1, the assessment process assigned the company a maturity level.

CMMC Certification Levels (Maturity Levels)

There are five CMMC levels. Each level has specific requirements:

Level 1: Basic cyber hygiene — Companies at level 1 perform basic cyber hygiene. Data must be error-free, and applications and information systems that store or process sensitive information like personally identifying information (PII) must have proper access

controls. Standard procedures like obscuring PII and data quality assurance help you comply with this level. The NIST guidelines offer 17 basic security controls for this level.

Level 2: Intermediate cyber hygiene — The next level involves 72 controls (including the level 1 controls); these comprise a little over half of all NIST 800-171 controls. At this stage, your company must protect FCI and CUI in a repeatable way. Auditing, media protection, backup and recovery, maintenance, and system integrity are important at this level. The major difference between levels 1 and 2 is the implementation of a plan and procedures for protecting data.

Level 3: Good cyber hygiene — Level 3 requires implementing 132 controls, spanning the entirety of the set laid out by NIST SP 800-171 for CUI. Companies at this level typically deal with controlled but unclassified information. It requires a strong plan to deal with cybersecurity threats and the means to carry it out through awareness, training and incident response.

Level 4: Proactive cyber hygiene — Level 4 requires demonstrated excellence in deploying 156 controls [under NIST and other sources](#). The 24 added from level 3 deal largely with vetting security practices: The company must regularly assess and revise its policies for maximum effectiveness, and higher management is kept updated on issues.

Level 5: Advanced cyber hygiene — Level 5 adds an additional 25 requirements related to advanced threat detection and protection; this level is required for companies dealing with highly desirable information. Companies need to deploy more sophisticated tools such as anomaly detection, and be able to flexibly respond to threats.

CMMC framework components, levels and domains

Getting up to speed with the CMMC requirements requires an understanding of 17 different domains. 14 of the domains come from Federal Information Processing Standards (FIPS) 200 and NIST SP 800-171; CMMC adds three more: recovery, situational awareness and asset management. Here is the complete list:

Access control — Know who has access to your systems and strictly limit access by job role.

Audit and accountability — Track users with access to sensitive data. Collect event logs and investigate the information for improper or suspicious activity.

Asset management — Track hardware and software assets to avoid allowing outdated and unwanted technology to lead to a data breach

Awareness and training — Provide regular training for employees on how to prevent breaches and how to respond if one occurs.

Configuration management — Establish baseline configurations that protect systems from unwarranted access, setting reasonable defaults to avoid exposing your company to threats.

Identification and authentication — Use authorization rules and practices, such as multi-factor authentication, to avoid exposure of mission-critical information.

Incident response — Create a plan for quickly investigating, reporting on and resolving security incidents.

Maintenance — Regularly patch and upgrade technologies and facilities to minimize vulnerabilities.

Media protection — Identify and protect media, and create protocols for sanitation and disposal.

Personnel security — Conduct appropriate personnel screening and background checks. Be ready to provide evidence that your CUI is protected during personnel actions like transfers or turnovers.

Physical protection — Protect your facilities, staff and systems from physical threats like unauthorized access, theft and damage.

Recovery — Set up a solid backup and recovery plan in the event of partial or total data loss.

Risk management — Periodically assess risks, develop strategies to counter them, and measure progress.

Security assessment — Assess security by reviewing previous audits, your risk management strategy, and other information.

Situational awareness — Implement real-time monitoring for your technologies and respond to threats appropriately.

System communications and protection — Define the security required to protect each system.

System and information integrity — Identify and manage flaws in systems, find hazards, and review network security for potential issues.

How can I get CMMC certification?

All defense contractors will need to undergo an official audit performed by an independent CMMC third-party assessor organization (C3PAO) or an individual certified by the DoD. The DoD does not accept a result from any other auditor. The [CMMC Accreditation Body](#) has more information on who is a certified auditor.

In general, a CMMC certificate will be valid for 3 years and will not be made public, but it will be posted on specific DoD databases. Recertification is required after this period of time or in the event of data loss.

A DIB company that suffers a cybersecurity incident won't lose its CMMC certification automatically. However, you must follow proper reporting procedures. Contact the DoD and prepare a thorough report of the incident detailing why it occurred and how such a breach can be prevented in the future.

How can I get ready for a CMMC certification audit?

A good guideline to follow when preparing for your audit is [Executive Order 13556](#), which standardizes how the executive branch deals with unclassified information that needs protection.

More broadly, consider using the following high-level checklist:

1. **Get advice from your federal or state agency.** Make sure you understand what's expected of you.

2. Audit your current data and technologies.

Gather as much information as you can on the current state of your security, including user access controls, software being used and available security procedures. Identify where you store, process or transmit CUI and FCI.

3. Build a solid plan. Next, create a solid CMMC compliance program or plan based on the level of certification you seek. For example, companies seeking the highest maturity levels will want to harden their networks and separate technologies dealing with highly sensitive information from the rest of their infrastructure.

4. Conduct a gap analysis. Assess your current cybersecurity maturity level and determine what you need to do to reach the appropriate level. Make the necessary changes based on the gap analysis.

5. Implement your policy. Train your staff and set dates to assess your organization as a whole. Persistence is the key to hardening your systems and promptly spotting and blocking attacks.

6. Hire a professional to oversee compliance. This individual will interact with your IT team to make sure all standards are met. They will also prepare evidence and documentation to

prove that your organization is protecting CUI.

7. Extend your review. Make sure all subcontractors, as well as everyone in your supply chain, are also compliant with NIST SP 800-171.

How does Netwrix help with CMMC compliance?

Using established best practices and understanding the compliance lifecycle is a good way to build a solid foundation for compliance with any standard, including the CMMC. With the [Netwrix Data Security Platform](#), you can achieve, maintain and prove compliance with less effort and expense. You can automate processes like [change, access and configuration auditing](#), ensure accurate [discovery and classification](#) of sensitive data, and get insights into your data and infrastructure security.

ON-DEMAND
WEBINAR

CMMC: Raise Your Cyber Maturity Level

Watch Now

Extra Security

NIST Cybersecurity Framework: Benefits and Key Components

Mike Tierney

VP of Customer Success,
Security and Compliance Expert

With cyber threats rapidly evolving and data volumes expanding exponentially, many organizations are struggling to ensure proper security. Implementing a solid cybersecurity framework (CSF) can help you protect your business.

One of the best frameworks comes from the National Institute of Standards and Technology. This guide provides an overview of the NIST CSF, including its principles, benefits and key components.

NIST Cybersecurity Framework Purpose and Benefits

The NIST Framework offers guidance for organizations looking to better manage and reduce their cybersecurity risk. It is important to understand that it is not a set of rules, controls or tools. Rather, it offers a set of processes that can help organizations measure the maturity of their current cybersecurity and risk management systems and identify steps to strengthen them.

Implementing the NIST cybersecurity framework is voluntary, but it can be immensely valuable to organizations of all sizes, in both the private and public sectors, for several reasons:

- It is easy to understand and use.
- It's meant to be customized — organizations can prioritize the activities that will help them improve their security systems.
- It is risk-based — it helps organizations determine which assets are most at risk and take steps to protect them first.

Benefits of NIST CSF

Use of the NIST CSF offers multiple benefits. In particular, it can help you:

- Gain a better understanding of current security risks
- Prioritize the activities that are the most critical
- Identify mitigation strategies
- Evaluate potential tools and processes
- Measure the ROI of cybersecurity investments
- Communicate effectively with all stakeholders, including IT, business and executive teams

Components of the NIST CSF

The NIST CSF includes three components:

- Core
- Implementation Tiers
- Profiles

Core

The core lays out high-level cybersecurity objectives in an organized way, using non-technical language to facilitate communication between different teams. At the highest level, there are five functions:

- **Identify** — Determining the cybersecurity risks to all company assets, including personnel, systems and information
- **Protect** — Implementing systems to safeguard the most vital assets
- **Detect** — Spotting active cybersecurity events that could pose a threat to your environment
- **Respond** — Taking action against threats to prevent or mitigate damage
- **Recover** — Restoring capabilities or services damaged by a threat

Each function is divided into categories, as shown below. There 23 NIST CSF categories in all.

Each category has subcategories — outcome-driven statements for creating or improving a cybersecurity program, such as “External information systems are catalogued” or “Notifications from detection systems are investigated.” Note that the means of achieving

each outcome is not specified; it’s up to your organization to identify or develop appropriate measures.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

NIST CSF Core Functions and Categories

Implementation Tiers

The NIST CSF has four implementation tiers, which describe the maturity level of an organization’s risk management practices. In other words, they help you measure your progress in reducing cybersecurity risks and assess whether your current activities are appropriate for your budget, regulatory requirements and desired risk level. The tiers are:

Tier 1: Partial — Informal, nonexistent or unsystematic risk management methods

Tier 2: Risk Informed — Partial, isolated implementation or unfinished risk management processes

Tier 3: Repeatable — Formal and structured policies and procedures and robust risk management programs

Tier 4: Adaptive — Responsive risk management programs that are continuously adapted and improved

Remember that it's not necessary — or even advisable — to try to bring every area to Tier 4. Instead, determine which areas are most critical for your business and work to improve those. NIST CSF suggests that you progress to a higher tier only when doing so would reduce cybersecurity risk and be cost effective.

Profiles

Profiles are essentially depictions of your organization's cybersecurity status at a moment in time. Organizations often have multiple profiles, such as a profile of its initial state before implementing any security measures as part of its use of the NIST CSF, and a profile of

its desired target state. These profiles help you build a roadmap for reducing cybersecurity risk and measure your progress.

Each profile takes into account both the core elements you deem important (functions, categories and subcategories) and your organization's business requirements, risk tolerance and resources. But profiles are not meant to be rigid; you may find that you need to add or remove categories and subcategories, or revise your risk tolerance or resources in a new version of a profile.

Getting Started with NIST Cybersecurity Framework

NIST offers an [Excel spreadsheet](#) that will help you get started using the NIST CFS. The spreadsheet can seem daunting at first. One way to work through it is to add two columns: Tier and Priority. In the Tier column, assess your organization's current maturity level for each subcategory on the 1–4 scale explained earlier. Use the Priority column to identify your most

important cybersecurity goals; for instance, you might rate each subcategory as Low, Medium or High. [This webinar](#) can guide you through the process.

As you move forward, resist the urge to overcomplicate things. Trying to do everything at once often leads to accomplishing very little. Remember that the framework is merely guidance to help you focus your efforts, so don't be afraid to make the CSF your own.

Also remember that cybersecurity is a journey, not a destination, so your work will be ongoing. With these lessons learned, your organization should be well equipped to move toward a more robust cybersecurity posture.

EBOOK

Kickstart Guide to Implementing the NIST Cybersecurity Framework

[Learn More](#)

Extra Security

Top Tactics for Preventing Data Leaks

Elena Vodopyan

Manager of Content Marketing

Data leaks don't get as much press as data breaches — but they can be just as devastating to your business. In this article, you'll learn how data leaks happen and the key steps to take to defend your organization.

What is a data leak? How does it differ from data breach?

A data breach occurs when an attacker from outside your organization gets into your IT ecosystem and steals private or sensitive information.

Data leakage, in contrast, happens from the inside out: Someone inside the organization shares confidential data with unauthorized recipients, or leaves a gap that enables that information to be easily accessed by people who shouldn't see it. Either action could be accidental or deliberate.

Like a data breach, a data leak can have multiple unpleasant consequences. It can result in lawsuits from the people whose data was exposed, penalties from regulatory agencies, and damage to your business reputation and bottom line.

What types of data can be leaked?

Obviously, data that is intended to be public cannot be leaked. This typically includes content like your organization's published press releases, product or service descriptions, and website privacy policy.

But most of the data that your organizations stores is not intended to be available to just anyone, and therefore can be improperly shared or accessed. Examples include:

- Trade secrets
- Source code
- Inventory information
- Research data
- Customer data (personal data, personal health information)
- Employee data (personal data, financial information, usernames & passwords)

How do data leaks happen?

Here are three of the most common causes of data leaks.

Misconfigurations by IT pros

In 2020, organizations around the globe rapidly transitioned to remote work. But when workers access proprietary tools and databases from home, any misconfiguration can put the data at risk. In fact, 60% of companies reported finding new security gaps because of the transition to remote work, according to the [Netwrix 2020 Cyber Threats Report](#).

Even industry-leading organizations have misconfigured systems in a way that left content vulnerable to data leakage. For example, [Microsoft](#) misconfigured security rules for a customer support case database, which left sensitive data exposed.

Malicious or careless business users

Data leaks can also be caused by malicious or careless employees who are not IT pros. Forrester predicts that [33% of data breaches](#) in 2021 will be caused by insider incidents—an increase from 25% in 2020. The company cites remote work as the reason for the uptick.

For example, Tesla found that a Quality Assurance software engineer stole thousands of files containing trade secrets by transferring

them to a personal Dropbox account. [Multiple healthcare providers](#) have experienced data leaks due to protected health information being accidentally sent to improper email recipients.

System errors

System or software issues are another common cause of data leakage. For example, a [software error in a Denmark government tax portal](#) exposed the tax ID numbers of 1.26 million Danish citizens over a period of five years. Each time a taxpayer updated their account details, an identifying number would be added to the page's URL, which would then be collected by Adobe and Google, which were running analytics on the site.

How do data leaks happen?

These five steps will help you strengthen security and prevent data leak problems:

1. Classify your data according to its value and sensitivity.

The first step in preventing data leaks is to know which data can be freely shared, and exactly who

should be allowed to access the other data you store. Using data discovery and classification, you can organize all your data into categories so you can protect it appropriately.

2. Proactively identify and mitigate IT risks.

You won't know where you're most vulnerable unless you regularly assess your risks. To implement effective risk assessment and risk management, consider using an industry standard like the assessment framework from the National Institute of Standards and Technology (NIST). The [NIST SP 800-30](#) document lays out the procedures for the assessment.

3. Protect your data according to its value and sensitivity.

Next, deploy the right security controls. The [NIST 800-53](#) standard can help you choose appropriate controls. Best practices include:

- Identity and access management (IAM), a framework that helps businesses implement and manage policies for access to sensitive information
- Encryption, which is the process of encoding data so that cannot be read even if it falls into the wrong hands
- Data access governance, which includes applying the principle of least privilege to ensure that users have only the access permissions they need to do their jobs

- Change management and auditing, which can help you avoid misconfigurations and other security gaps
- User and entity behavior analytics (UEBA), which helps you spot unusual activity that could lead to a data leak

4. Train all employees on security awareness.

[The Netwrix 2020 Cyber Threats Report](#) showed that 58% of companies are worried that their employees will ignore security rules, putting data at risk. To reduce the risk of costly mistakes, perform security training for all employees, including executives, on a regular basis.

5. Enable timely detection.

Detecting improper activity promptly can help you avoid or reduce the scope of a data leak. For example, alerts on changes to critical configuration parameters can enable you to immediately close a security gap, and spotting a user copying sensitive data to a local machine can enable you to intervene before the machine leaves the premises.

6. Be ready to recover.

Finally, a process must be put in place to recover any content that is lost in a data leak. Be sure to implement a test a thorough recovery plan for all important data.

How Netwrix can help you prevent data leaks

The [Netwrix Data Security Platform](#) can help you prevent data leaks. It provides all of the following essential capabilities:

- Automated [data classification](#) — Accurately identify and tag sensitive information across a wide range of on-prem and cloud-based data sources.
- [IT risk assessment](#) — Understand, prioritize and mitigate your IT-related risks.
- [IT auditing](#) — Detect threats, improve compliance and increase operational efficiency.
- User behavior analytics — Spot abnormal behavior before it leads to a data leak.

First-Hand Experience

Regional Council Eliminates Security Blind Spots and Reduces the Likelihood of a Breach

Queanbeyan-Palerang Regional Council is one of the fastest growing councils in the Southern Tablelands region of New South Wales, Australia. The Council is a progressive organization that is committed to continually improving its processes and services to provide increased value for the community.

Ensuring the continuity of public services and the safety of the data entrusted to the county is a top priority for the council's executive team. As a government entity, the council is a target for both intruders and malicious insiders. Therefore, establishing control over critical systems and gaining better insight into the activity of users was crucial.

In addition, the organization was eager to reduce IT workload and expenses by replacing the inefficient manual processes being used to conduct security investigations and enabling the IT team to quickly respond to critical or unwanted events that could pose a security threat.

To achieve those goals, the council knew it needed a solution would provide robust visibility and effective control over changes made across the entire IT environment.

Eliminating Security Blind Zones with a New Solution

When Bevan Hussey, Systems Officer at Queanbeyan-Palerang Regional Council, joined the organization, he recommended the IT auditing solution he'd used successfully at his previous job: Netwrix Auditor. This tool provides IT pros with control over key aspects of system security by providing visibility into effective permissions, control over access to files containing sensitive data and continuous monitoring of changes made to security configurations.

Mr. Hussey explained: "Why to go through a bunch of commands if there is Netwrix Auditor? It consolidates all information on activity and changes in your network in one place. It's great how easily you can retrieve information to investigate an incident or reply to an auditor's request."

Using Netwrix Auditor's access auditing capabilities, Mr. Hussey established strict control over user privileges to protect the council's critical data from insider and outsider threats and reduce the risk of human errors. At the same time, the tool's change auditing features give him a detailed picture of what is happening in the organization's critical IT systems, including Active Directory, Exchange, VMware and Windows Server. Moreover, its reporting and real-time alerting capabilities enable him to stay on top of all critical

changes, such as modifications to configurations, security settings and sensitive content.

As a result, Mr. Hussey can now ensure that changes are made only by authorized users and comply with established security policies. He also noted that the solution empowers him to improve IT staff education; for instance, if an admin accidentally adds a user to a privileged group or improperly revokes access rights, he can not only immediately detect and resolve the issue, but also provide additional training to the employee to prevent future mistakes.

To read the complete case study, please visit https://www.netwrix.com/success_story_qprc.html have maximum confidence in the organization, which is essential to its growth. In fact, the solution has proven to be such a valuable technology investment that Synergia Group is already planning to implement it at a third hospital.

To read the complete case study, please visit:
https://www.netwrix.com/success_story_qprc.html

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides.

Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

For more information visit www.netwrix.com

WHAT DID YOU THINK OF THIS CONTENT?



CORPORATE HEADQUARTER:

300 Spectrum Center Drive
Suite 200 Irvine, CA 92618

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:



netwrix.com/social