cybereason

7000+ IRs LATER

The 11 Essential Cybersecurity Controls

Decades in incident response reveal battle-tested cybersecurity controls that minimize attack surface, improve detection and response, reduce incident impact and losses, and build cyber resilience (with compliance mappings for easy implementation)

Threats grow in volume and sophistication, compliance frameworks get more stringent and complex, supply chain risk is ever-present, M&A activities introduce new issues… but cybersecurity budgets are stretched thin and experts struggle with burnout.

The cliché advice is to focus resources on the highest-impact projects, but which cybersecurity controls produce the highest returns?

Many security and risk leaders may cite popular cyber frameworks as their answer, as some organizations tend to rely on compliance frameworks to dictate priorities. Yet lots of technically compliant organizations suffer incidents. To address this gap, we set out to uncover the highest-impact controls that matter most during actual incidents, not just during audits.

INTRODUCING THE 11 ESSENTIAL CYBERSECURITY CONTROLS

In partnership with Intentional Cybersecurity and fueled by frontline intelligence from over 7,000 incident investigations, our experts have identified the 11 Essential Cybersecurity Controls representing the highest-impact, field-proven practices that reduce the likelihood, dwell time, and impact of cyber threats while enabling effective incident response and recovery.

Included within are common pitfalls for each control, highlighting misconfigurations and gaps we encounter most frequently, along with the direct impact each control has on digital forensics and incident response (DFIR) activities. The DFIR perspective, not present in any other framework, highlights the direct advantages of a successful control implementation.

> “After leading and overseeing thousands of cyber investigations worldwide, I’ve seen firsthand which defenses actually stop attackers and which ones routinely fail. The 11 Essential Cybersecurity Controls distill those hard-earned lessons into clear, prioritized actions that any organization can take to meaningfully reduce their risk.”

Devon Ackerman,
Global Head of DFIR, Cybereason

In partnership with INTENTIONAL CYBERSECURITY

MAKE THE MOST OF THE 11 ESSENTIAL CYBERSECURITY CONTROLS WITH A PRACTICAL CHEAT SHEET

We've created a desktop reference for the Essential Controls which you can download using this QR code

cybereason

7000+ IRs LATER

The 11 Essential Cybersecurity Controls

Decades in incident response reveal battle-tested cybersecurity controls that minimize attack surface, improve detection and response, reduce incident impact and losses, and build cyber resilience (with compliance mappings for easy implementation).

THE 11 ESSENTIAL CONTROLS WITH AN INCIDENT RESPONDER'S PERSPECTIVE

1. PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION (MFA)
Traditional MFA can be easily bypassed, so phishing-resistant MFA (such as FIDO2) is now essential. Well-implemented phishing-resistant MFA often stops attackers at the perimeter.

2. ENDPOINT DETECTION & RESPONSE (EDR)
When tuned and monitored, EDR is our fastest
tacker behavior. Weak
eaves blind spots.

ANAGEMENT (PAM)
r escalation and provides
vilege escalation is
pands exponentially.

& RETENTION (SIEM)
vestigator's backbone
rough EDR coverage.
ort-retention logs
nd accuracy.

ILITY MANAGEMENT
and timely, we see far
ons and unauthorized

6. EMAIL SECURITY & PHISHING PROTECTION
Phishing is the #1 intrusion vector. Strong controls eliminate entire attack paths; weak controls give attackers easy entry.

7. ASSET INVENTORY & VISIBILITY (IT, OT, CLOUD)
You can't investigate what you don't know exists. Missing inventory wastes time and lets attackers hide in shadow IT.

8. NETWORK SEGMENTATION, ACCESS CONTROLS
Segmentation provides natural containment boundaries. Without it, lateral movement becomes trivial and compounds risks to data.

9. IRP PLANS & TABLETOP EXERCISES
Practiced teams respond faster and more cohesively. Without rehearsals, chaos compounds incident damage.

10. DATA CLASSIFICATION & MANAGEMENT
When data is classified, we can quickly assess exposure and regulatory impact. Without it, extra time is consumed to find fundamental answers.

11. OFFLINE, SEGMENTED, TESTED BACKUPS
Tested offline backups remove leverage from ransomware actors. Unsegmented or untested backups often fail when needed most.

security Controls at
ntrols

Cybereason experts are available 24x7
response@cybereason.com

- **PRIORITIZE RESOURCES**
  Focus investments on the frontline-proven controls that actually stop incidents.
- **STRENGTHEN EXECUTIVE COMMUNICATION**
  Use the list to brief boards and justify security budgets with clarity.
- **IDENTIFY GAPS**
  Benchmark current defenses against the Essential Controls to find weaknesses fast.
- **ALIGN WITH INSURERS & RISK MANAGERS**
  Demonstrate maturity and reduce risk exposure with controls supported by the insurance market.
- **IMPROVE INCIDENT PREPAREDNESS**
  Run tabletop exercises around controls to validate resilience under pressure.
- **BRIDGE COMPLIANCE AND SECURITY**
  Translate checklists into real-world resilience by prioritizing high-impact controls.

TABLE OF CONTENTS

01 PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION (MFA)

MFA requires users to verify their identity using two or more authentication factors, typically something they know (password), something they have (device or token), or something they are (biometric), before accessing systems or applications. Traditional MFA can be easily bypassed using stolen credentials or token theft tactics, so the adoption of phishing-resistant MFA (such as FIDO2) is strongly recommended. In our investigations, attackers routinely gain access through compromised credentials or easily bypass traditional MFA using common phishing kits.

COMMON PITFALLS

Compromised accounts often do not have MFA implemented at all, and where it is enabled, it's only traditional MFA, which is commonly bypassed by threat actors leveraging phishing kits or social engineering tactics to capture both credentials and one-time tokens. Other common issues include relying solely on SMS-based MFA, failing to enforce MFA for all remote access paths (e.g., VPN, RDP, cloud admin portals), or allowing exceptions in security strictness for certain executive or privileged users.

DFIR PERSPECTIVE

The presence of properly enforced MFA often means attackers hit a wall after the initial compromise attempt. It gives incident responders fewer compromised accounts to investigate and helps isolate entry points. When MFA is weak or missing, lateral movement is easier, privilege escalation is faster, and the blast radius of successful compromises is broader. Properly implemented MFA also includes robust logging of threat actor activity, such as failed attempts and token reuse, allowing more precision and speed when pinpointing initial access or detecting adversary-in-the-middle phishing attempts.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	6.3 – Require MFA for External Applications 6.5 – Require MFA for Administrative Access
NIST CSF	PR.AC-7 – Users are authenticated commensurate with risk
NIST 800-171	3.5.3 – Use multifactor authentication for local and network access

02

ENDPOINT DETECTION AND RESPONSE (EDR) DEPLOYMENT

EDR solutions continuously monitor endpoint activity to detect, investigate, and respond to suspicious and anomalous behaviors like process injection, lateral movement, and credential harvesting across workstations, servers, and sometimes cloud workloads. EDR gives defenders near real-time and historical visibility into attacker behaviors. It's an essential tool for early detection and rapid containment, especially as adversaries use stealthy techniques that bypass traditional antivirus or perimeter defenses.

COMMON PITFALLS

Our incident data shows that most organizations have EDR in place, yet attackers still succeed in compromising their environments. The issue often isn't the tech, it's the investigative response. Most cases involved alert fatigue, lack of tuning, or missed detections due to weak triage processes. EDR agents may also be inconsistently deployed across endpoints, leaving gaps in visibility, particularly on legacy systems, cloud workloads, testing or development networks, or unmanaged devices (see control #7 for more details).

DFIR PERSPECTIVE

EDR is often our fastest path to understanding attacker behavior across a networked environment, from earliest activity, to lateral movement and privilege escalation attempts. When deployed and monitored correctly, EDR drastically reduces time to containment, but when coverage is incomplete or alerts are ignored, it slows investigations and leaves blind spots.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	10.1 – Deploy and Maintain Anti-Malware Software 13.1 – Centralize Security Event Alerting
NIST CSF	DE.CM-4 – Malicious code is detected RS.AN-1 – Notifications from detection systems are investigated
NIST 800-171	3.14.1 – Identify, report, and correct system flaws 3.14.5 – Perform periodic scans of information systems

03
PRIVILEGED ACCESS MANAGEMENT (PAM)

PAM limits and controls access to high-value systems, accounts, and data by enforcing just-in-time privileges, credential vaulting, session monitoring, and access approvals for administrative or sensitive functions. Privileged accounts are prime targets as they allow attackers to move laterally, disable defenses, or access sensitive data. Effective PAM restricts the blast radius of a compromise and can stop attackers from escalating to domain-wide control.

COMMON PITFALLS

Many organizations maintain overly generous admin rights across the network. Too many admin accounts, shared local admin accounts, admins with weak passwords and/or no MFA are common weaknesses. Others fail to rotate credentials, log privileged sessions, or audit who accessed what and when.

DFIR PERSPECTIVE

When PAM is enforced, we see a clear audit trail of privileged activity. It allows for streamlined containment, slowing attacker escalation, and lateral movement, thus giving us more time and visibility to detect and respond. Without PAM, attackers move faster (privilege escalations can be trivial), coverage gaps increase, and investigations take longer.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	4.3 – Configure Access Control for Admin Accounts 6.7 – Require Just-in-Time Privilege Elevation
NIST CSF	PR.AC-4 – Access permissions are managed PR.AC-6 – Identities are proofed and bound to credentials
NIST 800-171	3.1.2 – Limit system access to authorized users 3.1.6 – Use least privilege

04

CENTRALIZED LOGGING AND LOG RETENTION (SIEM OR EQUIVALENT)

Collecting and memorializing logs from operating systems, critical applications, and network and edge appliances, such as firewalls and VPNs, into a security information and event management (SIEM) or data lake platform is crucial for incident response investigations as well as regulatory compliance and overall cyber resilience. SIEM-like platforms allow deep analysis, which fuels faster detections and forensic investigations. Without centralized logging, meaningful patterns are missed, forcing incident responders to pursue other log sources or limit the investigation scope to the available evidence.

COMMON PITFALLS

One of the biggest issues we see is gaps in coverage. Critical logs (like PowerShell, authentication events, or cloud admin actions) are often missing. Others collect logs, but retain them for too short a time. Alerting rules may also be poorly tuned, leading to alert fatigue or blind spots. Pricing is a valid concern when it comes to logging, as it can be cost-prohibitive to ingest high volumes of data, so having an expert guide your logging and retention policy is encouraged.

DFIR PERSPECTIVE

Centralized logs are our investigation backbone. They help us reconstruct timelines, identify Patient Zero, and correlate attacker actions across systems. When logs are missing or siloed, our work becomes slower and less precise. Proper log retention and visibility directly influence the speed and depth of our response.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	8.2 – Enable Audit Logging 8.3 – Collect Detailed Audit Logs 8.5 – Retain Audit Logs for a Defined Period
NIST CSF	DE.AE-3 – Event data are aggregated and correlated PR.PT-1 – Audit/log records are determined, documented, implemented
NIST 800-171	3.3.1 – Create and retain system audit logs 3.3.6 – Provide audit reduction and report generation

05
REGULAR PATCHING & VULNERABILITY MANAGEMENT

This control focuses on identifying, prioritizing, and remediating vulnerabilities through regular system patching, configuration management, and security updates across endpoints, servers, network appliances, and applications. Unpatched vulnerabilities are one of the most reliable entry points for attackers. In our investigations, exploited vulnerabilities consistently appear in the top three initial access methods. Timely patching reduces the attack surface and blocks opportunistic intrusions before they begin.

COMMON PITFALLS

Organizations often lack an up-to-date asset inventory, which leads to blind spots (see control #7). Patching cycles may be slow or exclude high-risk categories, not due to the CVE scale, but to the likelihood of exploitability of the vulnerability. Even worse, some rely on vulnerability scans without timely, business reinforced remediation plans, or fail to track patch status across hybrid environments where one scanning tool may not support all devices or attack surfaces. Risk-based prioritization is rarely applied, so high-impact CVEs get buried under noise.

DFIR PERSPECTIVE

When patching and vulnerability management are mature, we encounter fewer preventable incidents. It also streamlines investigations so our team wastes less time chasing exploits of known, years-old CVEs. When it's weak, attackers gain fast access and pivot quickly, sometimes exploiting public exploits long after patches are available.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	7.3 – Apply Vendor-Supplied Updates 7.5 – Automate Patch Management
NIST CSF	PR.IP-12 – Vulnerability management plans are developed and implemented DE.CM-8 – Vulnerability scans are performed
NIST 800-171	3.11.2 – Scan for vulnerabilities 3.14.1 – Identify, report, and correct system flaw

06 EMAIL SECURITY FILTERING & PHISHING PROTECTION

This control includes technologies and processes to detect and block malicious emails, including phishing, malware, and spoofed domains. It typically combines secure email gateways, DNS filtering, DMARC enforcement, and user reporting mechanisms. Phishing and social engineering are the top initial intrusion vector in Cybereason IR cases, accounting for 46% of intrusions during H1 2025. Effective email security blocks many threats before they reach users and helps reduce credential theft, malware delivery, and business email compromise.

COMMON PITFALLS

Over time, email filters are often tuned too loosely, allowing advanced phishing emails to slip through. If a domain does not have DMARC configured at an enforcement level, or if SPF and DKIM are missing or misaligned with the domain's From address, the domains may remain vulnerable to spoofing. User reporting workflows are frequently broken or ignored, and phishing simulations are inconsistent or absent. Finally, email security is often siloed from broader incident detection systems.

DFIR PERSPECTIVE

Strong email controls can eliminate entire intrusion paths. When in place, we see fewer successful phishing-based compromises, which limits both initial access and lateral movement. When missing, phishing gives attackers credentials, payload delivery opportunities, or persistence before they ever touch your endpoints. Coupled with control #4, email security solutions also generate valuable logs that assist investigators to trace the attack, confirm who was targeted, and pinpoint data at risk.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	9.1 – Ensure Email Server is Configured to Block Phishing 9.2 – Use DNS Filtering Services 14.6 – Train Workforce on Recognizing and Reporting Phishing
NIST CSF	PR.AT-1 – All users are trained DE.CM-7 – Monitoring for unauthorized mobile code or email attachments PR.DS-2 – Data in transit is protected (email encryption)
NIST 800-171	3.1.17 – Protect email from unauthorized access 3.13.8 – Implement email protection mechanisms 3.2.1 – Ensure personnel are trained to recognize threats (e.g., phishing)

07 ASSET INVENTORY & VISIBILITY (IT, OT, CLOUD)

Maintaining a current and accurate inventory of all hardware, software, virtual machines, cloud services, and OT/IoT assets across the organization is crucial. Visibility should include asset attributes, status, ownership, and security posture, regardless of product or scanning platform. You can't secure what you can't see. Attackers exploit unmanaged, unknown, or unmonitored systems, especially in hybrid IT/OT and cloud-heavy environments. Asset visibility is foundational for patching, access control, incident detection, and response.

COMMON PITFALLS

Inventories are often incomplete, manually maintained, or siloed between Network Engineering, IT, InfoSec, and Development and Production teams. Shadow IT often creates preventable blind spots. Many organizations don't tag assets by criticality, data contained within, dependencies, or owner, making it difficult to prioritize response or more immediately understanding what is at risk when unauthorized access has occurred. Discovery tools may lack integration or fail to scan beyond core infrastructure.

DFIR PERSPECTIVE

In an investigation, knowing what systems exist and where they live drastically improves scoping and containment. When inventories are incomplete, we waste time chasing unknown endpoints or cloud resources the client didn't even know they had. Good asset visibility also helps us correlate alerts and logs more accurately.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	1.1 – Establish and Maintain Detailed Enterprise Asset Inventory 1.2 – Address Unauthorized Assets 2.1 – Establish and Maintain Software Inventory
NIST CSF	ID.AM-1 – Physical devices and systems are inventoried ID.AM-2 – Software platforms and applications are inventoried ID.AM-4 – External information systems are catalogued
NIST 800-171	3.4.1 – Establish and maintain baseline configurations and inventories 3.1.1 – Limit access to authorized users, processes, or devices based on inventory

08 NETWORK SEGMENTATION & ACCESS CONTROLS

Dividing networks into isolated zones based on sensitivity, business function, or trust level, and enforcing access controls between them makes it harder for attackers to move past the initial compromise. Commonly accomplished with firewalls, access control lists, virtual local area networks, or cloud-native segmentation, it limits blast radius, protects crown jewels, and slows down adversaries. Access controls ensure that only the right systems, service, or user accounts can reach sensitive zones or services. As such, access controls are the foundation of identity-based access enforcement and implementation and required for successful privileged access management (see control #3).

COMMON PITFALLS

Many networks are still overly permissive, with broad internal access and little segmentation between critical systems and general-purpose user networks. Firewall rules are outdated or “allow any” by default. In cloud environments, overly broad identity and access management roles or security group misconfigurations are common. Segmentation often focuses on the external perimeter, but neglects internal lateral movement paths.

DFIR PERSPECTIVE

Segmentation gives us natural boundaries for containment. When it’s enforced, an attacker may compromise a user machine, but is unable to reach segmented zones for specific business functions such as finance, human resources, IT management, or backup environments. Without it, lateral movement is fast and wide-reaching, and our IR team has to isolate entire environments during investigations, rather than just a few segments.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	3.3 – Configure Firewall Rules Based on Traffic Filtering Needs 14.4 – Segment Administrative and Privileged Access 12.1 – Centralize Infrastructure Access Control
NIST CSF	PR.AC-5 – Network integrity is protected PR.PT-4 – Communications and control networks are protected
NIST 800-171	3.1.3 – Control flow of CUI in accordance with approved authorizations 3.1.20 – Verify and control connections to external systems

09 INCIDENT RESPONSE PLANS (IRP) & TABLETOP EXERCISES

This control involves developing a formal incident response plan (IRP) that outlines roles, responsibilities, communication protocols, and technical procedures for responding to cyber incidents. Tabletop exercises are then structured to test and refine IRPs in simulated attack scenarios. In a crisis, lack of coordinated response costs time. A well-practiced IR plan improves coordination, speeds up containment, and reduces business impact. Tabletop exercises uncover process gaps, validate assumptions, and strengthen relationships across legal, IT, PR, and leadership teams before an actual intrusion occurs.

COMMON PITFALLS

Many plans are outdated, untested, or written for compliance checkboxes. They're often too technical or too vague, with no clear ownership of decisions like whether to notify regulators or pull the plug on a system. Tabletop exercises, if done at all, may be overly scripted or exclude key stakeholders like legal, PR, or executives. Lessons learned are not often captured or acted on.

DFIR PERSPECTIVE

Organizations that have practiced incident response at least once respond faster and more cohesively. We spend less time waiting for access or approval and more time containing the intrusion event. When there's no plan or the team hasn't rehearsed, response is chaotic, and that chaos compounds the damage.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	17.1 – Designate Personnel to Manage Incident Handling 17.2 – Establish and Maintain Contact with Authorities 17.4 – Conduct Routine Incident Response Exercises
NIST CSF	RS.RP-1 – Response plan is executed during or after an incident RS.IM-1 – Response strategies are tested and updated IM.RM-1 – Risk management processes are established and practiced
NIST 800-171	3.6.1 – Establish incident-handling capability 3.6.2 – Track, document, and report incidents 3.6.3 – Test the organizational incident response capability

10
DATA CLASSIFICATION & STRUCTURED DATA MANAGEMENT

Identifying and categorizing data based on sensitivity, value, and regulatory requirements, and implementing controls to manage, protect, and govern data throughout its lifecycle helps prioritize protections, drive access controls (see control #8), and inform incident response and regulatory obligations. Attackers quickly find file servers, databases, and SharePoint folders containing intellectual property, financials, PII, etc. Knowing where that data lives and how it's protected is critical to reducing risk.

COMMON PITFALLS

Many organizations don't know where their sensitive data resides, or data classification efforts may be manual, static, or disconnected from actual security controls. Structured data (e.g., databases) may be governed, but unstructured data (e.g., file shares, cloud storage) often lacks oversight. Tagging, encryption, and retention policies may be missing or inconsistently applied.

DFIR PERSPECTIVE

When data is well-classified, we can quickly understand what's at risk during an incident and advise on necessary notifications and legal exposure. Without it, IR teams often have to spend valuable hours figuring out whether attackers accessed regulated or high-value data. To make it more realistic: if you know an attacker only encrypted the server where you store marketing collateral, would you pay the ransom?

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	3.4 – Use Automated Tools to Inventory Data 3.6 – Encrypt Sensitive Data in Transit 3.7 – Establish Data Classification Scheme
NIST CSF	ID.RA-1 – Asset vulnerabilities are identified and documented PR.DS-1 – Data-at-rest is protected PR.DS-5 – Protections against data leaks are implemented
NIST 800-171	3.1.22 – Control CUI posted or processed in public systems 3.8.1 – Protect CUI in accordance with flow restrictions 3.8.3 – Mark and label CUI appropriately

11

OFFLINE, SEGMENTED, & TESTED BACKUPS WITH RTO VALIDATION

In the ideal implementation of immutable backups, a data copy exists that cannot be modified, deleted, or encrypted by anyone, even an administrator or a compromised system, for a set retention period. While having immutable, segmented backups is a critical last line of defense in ransomware scenarios, it should not be the first or only focus. Backups support recovery italicize after an incident, but the other 10 controls are more impactful in preventing and containing attacks italicize before they cause damage.

COMMON PITFALLS

Backups are often online and accessible from the same network as production systems, making them just as vulnerable during an attack. In some cases, backups exist, but haven't been tested or fail to meet the actual recovery time objective (RTO) needs. Organizations may focus on backup frequency, but not test how fast they can actually restore (RTO). In addition, recovery processes are rarely rehearsed under data encryption or destruction events like ransomware or system-wide compromise conditions.

DFIR PERSPECTIVE

We frequently see cases where recovery is delayed or impossible because backups were encrypted or deleted by the attacker. Offline, segmented backups remove a lot of leverage from ransomware actors and gives leadership more options. Recovery time and effectiveness are dramatically better in those environments.

FRAMEWORK	CONTROL COMPLIANCE MAPPING
CIS v8	11.4 – Protect Recovery Data 11.5 – Ensure Regular Automated Backups 11.6 – Perform Periodic Restoration Tests
NIST CSF	PR.IP-4 – Backups are performed, protected, and tested PR.PT-5 – Recovery processes are tested RC.RP-1 – Recovery plan is executed and maintained
NIST 800-171	3.6.1 – Establish incident-handling capability (supports recovery) 3.6.2 – Track, document, and report incidents (including recovery) 3.1.1 – Limit system access, including access to backups

cybereason

TAKE THE NEXT STEP IN CYBER RESILIENCE

Our experts have responded to thousands of incidents and can help you benchmark your security program against the 11 Essential Controls.

Schedule a 1:1 session with a Cybereason expert today via **response@cybereason.com**.

THE IR TEAM *YOU TRUST*

7,000+	**300+**	**500+**	**100+**
Incidents investigated	Elite experts	Tabletops orchestrated	Certifications including CREST, SANS, OSCP