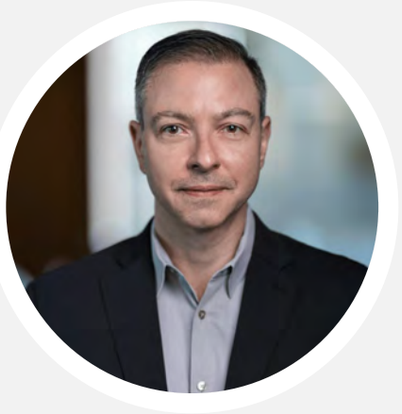
coretelligent

Cyber Security Checklist

9 ways to take charge of your cyber defense – and increase your business survivability



The luxury of treating cyber security as strictly an IT concern is one that businesses can no longer afford. Sophisticated cyber threats are evolving daily, and even a single successful attack can have devastating consequences for a business's bottom line and reputation.

Consider these statistics from the latest FBI Internet Crime Report. In 2023 alone, U.S. businesses filed:

- 21,489 complaints about Business Email Compromise (BEC) scams, amounting to $2.9 billion in losses; and
- 2,825 complaints about ransomware incidents – an 18% increase from 2022 – with reported losses jumping 74% to $59.6 million.

And those are just two data points in the roiling universe of today's alarming threat landscape. The stream of reports is relentless: Cyber criminals are targeting organizations of all sizes, exploiting vulnerabilities, and leveraging advanced tactics to disrupt operations, steal sensitive data, and extort money. The impacts of such attacks – which range from operational downtime and lost productivity to regulatory fines and reputational damage – can jeopardize any company's profitability, market position, and long-term sustainability.

Fortunately, there are actionable steps you can take immediately to protect your business from the bad actors now flooding the digital marketplace.

We created this Cyber Security Checklist to walk you through the foundational elements every business needs in order to mount a vigorous cyber security defense. While not intended as exhaustive, this checklist offers a way to benchmark your status – or help build your to-do lists – around nine critical defense components in three categories: People, Technology, and Processes.

Jason Baron

Chief Technology Officer, Coretelligent

Cyber Security Master Checklist

Brought to you by Coretelligent

Use this master checklist to assess your organization's status on our 9 foundational cyber security best practices. There are also individual best practice checklists included in each section.

People

Develop the right business–cybersecurity mindset

IT Steering Committee

- [ ] In place & active
- [ ] In progress
- [ ] To-do

Security Awareness User Training

- [ ] In place & active
- [ ] In progress
- [ ] To-do

Access Reviews

- [ ] In place & active
- [ ] In progress
- [ ] To-do

Technology

Amplify your ability to make security more effective

Mandatory MFA

- [ ] In place & active
- [ ] In progress
- [ ] To-do

Email Security

- [ ] In place & active
- [ ] In progress
- [ ] To-do

Endpoint Detection and Response (EDR)

- [ ] In place & active
- [ ] In progress
- [ ] To-do

Processes

Keep your business operating securely

Backup and Recovery

- [ ] In place & active
- [ ] In progress
- [ ] To-do

Incident Response Plan

- [ ] In place & active
- [ ] In progress
- [ ] To-do

TPRM / Vendor Management

- [ ] In place & active
- [ ] In progress
- [ ] To-do

People

Develop the right business–cybersecurity mindset

- IT Steering Committee
- Security Awareness User Training
- Access Reviews

IT Steering Committee

An IT Steering Committee is a cross-functional team that's responsible for aligning your IT initiatives with your business objectives. They provide governance and oversight for your IT strategy and investments – including cyber security programs, policies, and projects.

Key roles to involve in your IT Steering Committee include:

- **CEO or COO**
  Someone to provide the business vision
- **CIO, CTO, CISO, or IT Leader**
  Someone to provide technical expertise and IT strategy
- **Key Business Leaders**
  To provide relevant operational insights
- **CFO**
  Someone to offer input on budgetary prioritie
- **HR Leader**
  Someone to offer perspective on training and hiring needs

Timing Best Practice

Quarterly or bi-annual meetings should be held to review and adjust IT strategies and priorities.

Why This Belongs in Your Cyber Security Toolkit

- Ensures executive buy-in and support for cyber security initiatives.
- Provides oversight and accountability that keep cyber security initiatives aligned with strategic business goals.
- Helps head off friction between conflicting security and operational mandates when creating things like acceptable use policies, data protection standards, and incident response procedures.
- Creates an open forum for raising concerns and collaborating on cyber security decisions.

IT Steering Committee Checklist

01

Make sure your committee has the full picture of your IT ecosystem by involving a diverse cross-section of business units and stakeholders.

- [ ] Done
- [ ] In progress
- [ ] To-do

02

Clearly define committee roles, responsibilities, and decision-making processes.

- [ ] Done
- [ ] In progress
- [ ] To-do

03

Establish cyber security resource assignment as a requirement for all IT initiatives.

- [ ] Done
- [ ] In progress
- [ ] To-do

04

Regularly review and prioritize IT projects to keep up with changes in strategic importance, evolving cyber threats, and potential business impact.

- [ ] Done/process in place
- [ ] In progress
- [ ] To-do

Security Awareness User Training

Security Awareness User Training involves educating employees about critical cyber security best practices, potential threats, and their role in protecting your organization's data and systems.

Key topics to cover in your Security Awareness User Training include:

- **Phishing Attacks**
  How to identify and avoid falling for suspicious emails
- **Social Engineering**
  What to know about user manipulation techniques like deepfakes, impersonation, pretexting, and baiting
- **Password Security and Authentication**
  How to create and manage strong passwords and the importance of multi-factor authentication
- **Malware and Ransomware**
  How to have safe browsing habits and follow best practices around links and attachments
- **Data Protection and Privacy**
  How to securely handle sensitive customer and employee data, including specific training on compliance requirements
- **Physical Security**
  Things like not tailgating or propping open secure doors, protecting devices from theft, and maintaining a clean desk policy
- **Incident Response**
  What to do in the event of a cybersecurity incident, from how to report events to steps they can take to mitigate the impact
- **Mobile and Remote Security**
  Best practices around mobile devices, using public Wi-Fi, and remote access to company resources

Timing Best Practice

Ongoing training should be conducted at least annually, with regular refresher sessions and updates to address emerging threats and changes in the cyber security landscape.

Why This Belongs in Your Cyber Security Toolkit

- People are one of the weakest links in your cyber security armor. According to the Verizon 2024 Data Breach Investigations Report, "the human element was a component of 68% of breaches."
- Regular training creates a cybersecurity-conscious culture where following best practices becomes muscle memory.
- Industry regulations and standards like HIPAA, PCI DSS, and GDPR require you to provide security awareness training for employees handling sensitive data.

Security Awareness User Training Checklist

01

Establish – or work with an IT partner with advanced capabilities to develop – a security training program tailored to your specific processes, vulnerabilities, and requirements.

- [ ] Done
- [ ] In progress
- [ ] To-do

02

Customize training content to ensure practical relevance for different roles and responsibilities.

- [ ] Done
- [ ] In progress
- [ ] To-do

03

Incorporate interactive elements, such as simulated phishing and tabletop exercises, to reinforce learning.

- [ ] Done
- [ ] In progress
- [ ] To-do

04

Regularly assess the effectiveness of the training program and adjust as needed.

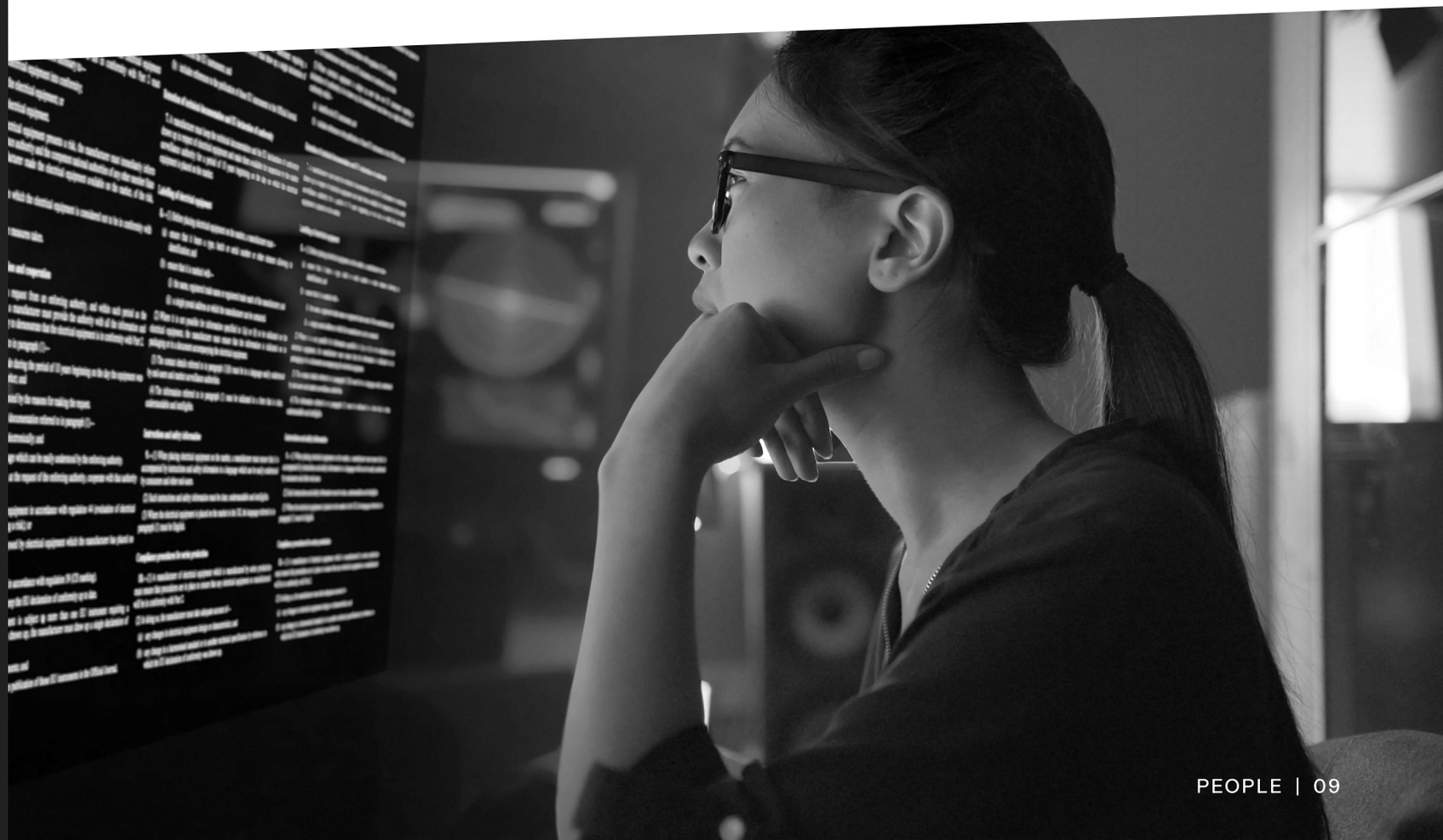
- [ ] Done/process in place
- [ ] In progress
- [ ] To-do

Access Reviews

Access Reviews are a process for ensuring that systems and data access permissions for all employees and third-party vendors are appropriate for their specific roles and responsibilities.

Key Access Review activities for each employee and vendor include:

- **Granting Access**
  As part of onboarding
- **Modifying access**
  As responsibilities change
- **Revoking access**
  As part of offboarding or termination



Timing Best Practice

Conduct reviews at least annually, with additional access reviews triggered automatically by role and status changes.

Why This Belongs in Your Cyber Security Toolkit

- Satisfies compliance requirements for access control to sensitive data, as specified in standards like HIPAA, PCI DSS, SOX, and ISO 27001.
- Addresses privilege creep (accumulating excessive permissions over time) and orphaned accounts (overlooked accounts that remain active after an employee leaves your organization or vendors are terminated).
- Reduces your attack surface and makes it more difficult to infiltrate your systems.
- Stops data breaches and IP theft by detecting unusual access patterns, privilege abuse, or unauthorized activities.
- Promotes organization-wide awareness that system access is being monitored and reviewed.

Access Reviews Checklist

01

Assess user access risks based on levels of privilege, potential for systems and data misuse, and impact if their access is compromised.

- [ ] Done
- [ ] In progress
- [ ] To-do

02

Establish a clear hierarchy of access levels based on job function.

- [ ] Done
- [ ] In progress
- [ ] To-do

03

Implement a formal process for modifying and revoking access rights according to changes in roles and responsibilities.

- [ ] Done
- [ ] In progress
- [ ] To-do

04

Continuously monitor, review, and audit user access rights to identify and address any discrepancies or unnecessary permissions.

- [ ] Done/process in place
- [ ] In progress
- [ ] To-do

05

Prioritize access reviews for high-risk users and critical systems and data.

- [ ] Done
- [ ] In progress
- [ ] To-do

06

Maintain detailed documentation of access rights and changes for audit and compliance purposes.

- [ ] Done/process in place
- [ ] In progress
- [ ] To-do

Technology

Amplify your ability to make security more effective

- → Mandatory MFA
- → Email Security
- → Endpoint Detection and Response (EDR)

Mandatory MFA

Mandatory Multi-Factor Authentication (MFA) is a security measure that requires users to provide two or more forms of identity verification in order to access systems, applications, or data.

Three common MFA variables that can be combined to verify a user's identity are:

- **Something they know**
  Such as a password, PIN, or answer to a security question
- **Something they possess**
  Such as a token, mobile app, or one-time use code texted to their phone
- **Something they are**
  Such as a unique physical characteristic like a fingerprint, handprint, or iris pattern, which can be used for biometric identity verification

Timing Best Practice

There's no set best practice for how frequently user prompts should be updated. We recommend:

1. periodic reviews to ensure the effectiveness of authentication methods used; and
2. setting different MFA prompt frequencies based on the risk level of the user, account type (i.e., admin versus standard user), or service being accessed.

Why This Belongs in Your Cyber Security Toolkit

- ➜ Offers an added layer of security against unauthorized access, even if passwords are compromised.
- ➜ Mitigates risks associated with employees using unmanaged devices to perform work over unsecured networks.
- ➜ Serves as an additional warning system by alerting legitimate users of unauthorized access attempts.
- ➜ According to Microsoft's Digital Defense Report, attempted password attacks increased "more than tenfold in 2023, from 3 billion per month to more than 30 billion per month."

Mandatory MFA Checklist

01

Work with your IT team or IT services partner to implement MFA for all user accounts.

- ☐ Done
- ☐ In progress
- ☐ To-do

02

Customize authentication factor requirements based on the level of risk and sensitivity of the data or systems being accessed.

- ☐ Done
- ☐ In progress
- ☐ To-do

03

Provide user training and support to ensure proper understanding and adoption of MFA.

Pro tip: For a helpful visual that compares the strength of different access security methods, see renowned cyber security expert Daniel Miessler's Consumer Authentication Strength Maturity Model infographic.

- ☐ Done/Process in place
- ☐ In progress
- ☐ To-do

04

Regularly review and update MFA configurations to address evolving vulnerabilities and threats.

- ☐ Done/Process in place
- ☐ In progress
- ☐ To-do

Email Security

Email Security encompasses a range of tools and tactics designed to protect your digital communications from threats like phishing, spam, malware, and data leaks.

Key technology approaches to securing your business email include:

- **Sender Authentication**
  Verify sender identity using techniques like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting & Conformance (DMARC) to detect spoofing.
- **Message Encryption**
  Use technologies like S/MIME (Secure/Multipurpose Internet Mail Extension) and PGP (Pretty Good Privacy) to enable secure email transmissions.
- **Virus/Malware Scanning**
  Scan emails and attachments for known viruses, malware, or other malicious content.
- **Blacklisting/Blocklisting**
  Block email traffic from known spam sources or IP addresses on a blacklist.
- **Greylisting/Whitelisting**
  Temporarily block and allow emails based on sender reputation or approved sender lists.
- **Content Filters**
  Analyze email content (text, images, attachments) for spam signatures, keywords, or other spam indicators using techniques like Bayesian filters.
- **URL/Link Analysis**
  Scan URLs/links in emails for signs of common indicators of phishing campaigns, things like suspicious domains and redirects.

Timing Best Practice

Email security tactics and strategy need to be continuously monitored, frequently tested, and updated to ensure effectiveness and alignment with things like email provider policies, regulatory changes, and threat landscape shifts.

Why This Belongs in Your Cyber Security Toolkit

- Helps thwart attackers from exploiting one of the most convenient entry points into your most critical systems and data.
- According to Microsoft's Digital Defense Report 2023, scammers' business email compromise (BEC) attacks skyrocketed to over 156,000 attempts between April 2022 and April 2023. Common BEC activities include:
  - Impersonating legitimate third-party domains to trick users into making fraudulent wire transfers.
  - Using employees' compromised credentials to launch internal phishing attacks.
  - Auto-subscribing users to lists and newsletters in order to trigger an avalanche of emails ("sometimes exceeding 1,000 per minute"), causing victims to miss authentication and warning messages in the chaos.

Email Security Checklist

01

Implement email filtering and anti-spam solutions to block known threats and suspicious emails.

- [ ] Done
- [ ] In progress
- [ ] To-do

02

Deploy email encryption and data loss prevention (DLP) tools to protect sensitive information in email communications.

- [ ] Done
- [ ] In progress
- [ ] To-do

03

Implement DMARC to authenticate outgoing emails and prevent domain spoofing.

- [ ] Done
- [ ] In progress
- [ ] To-do

04

Provide user training on identifying and reporting suspicious emails or phishing attempts and offer strategies and tools that help change employees' risky email behaviors.

- [ ] Done/Process in place
- [ ] In progress
- [ ] To-do

05

Regularly review and update email security configurations and policies to address emerging threats.

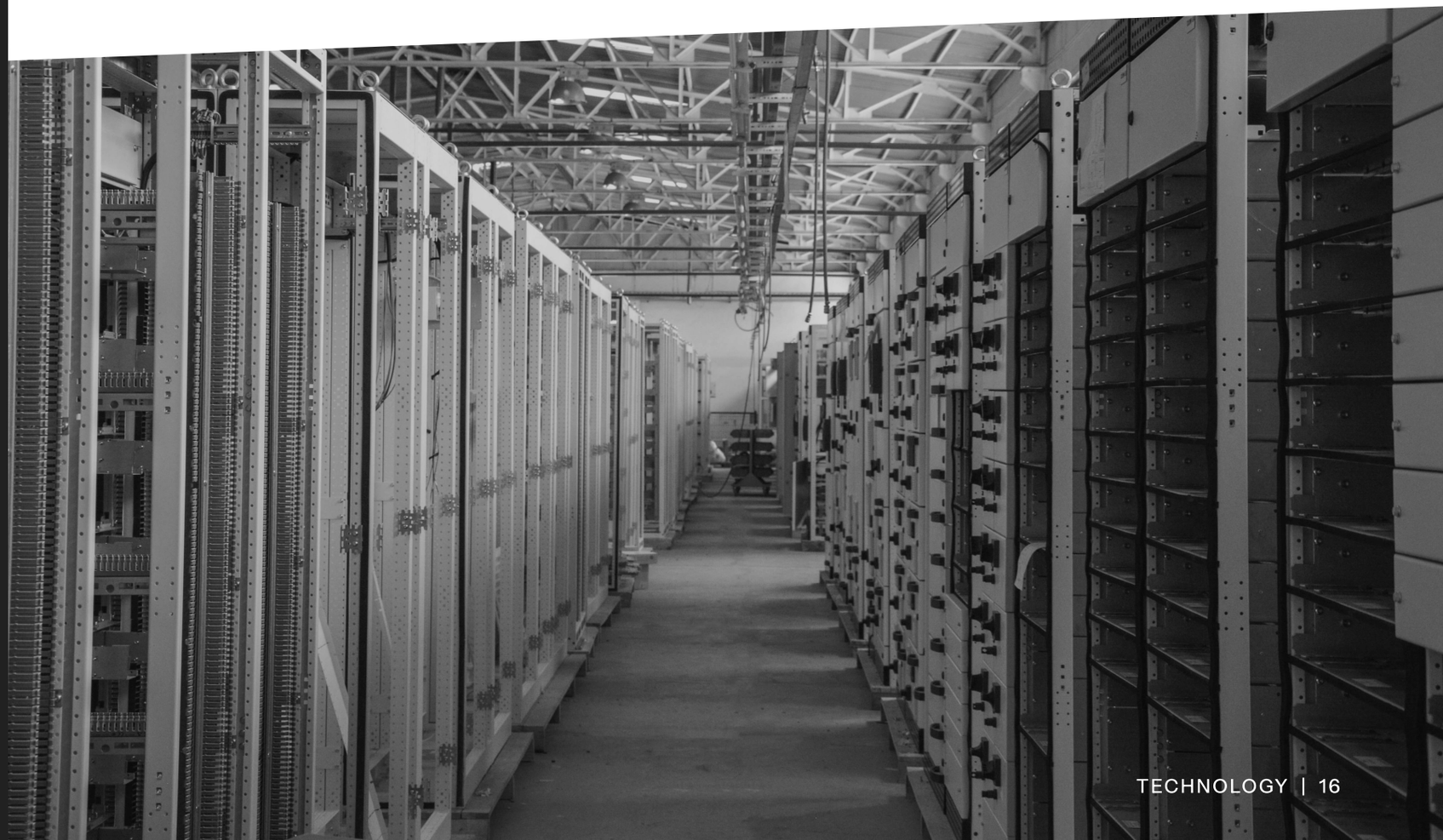
- [ ] Done/Process in place
- [ ] In progress
- [ ] To-do

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) is a modern technology that, unlike traditional antivirus solutions, proactively monitors and collects data from endpoints (e.g., laptops, desktops, servers) to shut down advanced security threats in real time.

Key elements of EDR solutions include things like:

- Behavioral analysis to identify suspicious patterns and indicators of attack
- Automated response capabilities like isolating compromised devices, terminating malicious processes, and quarantining infected files
- Integrated threat intelligence feeds that help you correlate activities with known threat indicators and attribute attacks to specific threat actors
- Incident triage, investigation, and reporting tools



Timing Best Practice

EDR updates are typically vendor-driven. Ask your EDR provider to share their update frequency and how they address evolving threats and vulnerabilities.

Why This Belongs in Your Cyber Security Toolkit

- Quickly identifies and mitigates threats before they can cause significant damage.
- Doesn't rely on known signatures, making it more effective than traditional antivirus solutions against advanced threats and zero-day attacks.
- According to Microsoft's Digital Defense Report 2023, 80–90% of all successful ransomware compromises originate through unmanaged devices.

EDR Checklist

01

Implement an EDR solution that integrates with your existing security infrastructure and policies, and provides comprehensive endpoint visibility.

- [ ] Done
- [ ] In progress
- [ ] To-do

02

Regularly review and analyze EDR data and alerts to identify potential threats and improve detection capabilities.

- [ ] Done/Process in place
- [ ] In progress
- [ ] To-do

03

Ensure that your EDR solution is regularly updated with the latest threat intelligence and detection capabilities.

- [ ] Done/Process in place
- [ ] In progress
- [ ] To-do

04

Confirm that your security teams have enough training and support to effectively manage your EDR solution.

- [ ] Done/Process in place
- [ ] In progress
- [ ] To-do

Processes

Keep your business operating securely

- → Backup and Recovery
- → Incident Response Plan
- → TPRM / Vendor Management

Backup and Recovery

Backup and Recovery processes enable you to create and maintain copies of critical data and systems to ensure their availability and integrity in case of system failures or cyber attacks.

Key backup and recovery strategies enable you to use different solutions for different types of data:

- **Full backup**
  Complete copy of all data, including all previous versions, at a given point in time
- **Incremental backup**
  Backs up only the data that has changed since the last backup activity (full or incremental)
- **Differential backup**
  Backs up only the data that has changed since your last full backup
- **Mirror backup**
  Comparable to a full backup, but saves only the latest version
- **Synthetic full backup**
  Combines the latest full backup with subsequent incremental backups to create a new full backup
- **Continuous data protection**
  Continuously captures and saves data changes to enable recovery to any point in time

Timing Best Practice

Backup frequency should be determined by the criticality of the data and systems involved. Recovery processes should be tested at least annually, as well as after any significant IT changes.

Why This Belongs in Your Cyber Security Toolkit

- Helps you satisfy compliance requirements that explicitly mandate robust backup and recovery capabilities. Examples include HIPAA, GDPR, NYDFS, DORA for EU financial entities, SOX, and PCI DSS.
- Helps you achieve information security and data protection certifications like ISO 27001 and SOC 2.
- Minimizes disruptive and costly downtime.
- Safeguards critical business data from loss, corruption, and ransomware attacks.
- Prevents customers from defecting to competitors who remain operational during incidents.

Backup and Recovery Checklist

01

Identify and prioritize critical data and systems that require backup and recovery processes.

- [ ] Done
- [ ] In progress
- [ ] To-do

02

Implement a comprehensive backup strategy for each priority level to ensure appropriate redundancy and availability.

- [ ] Done
- [ ] In progress
- [ ] To-do

03

Develop and document detailed recovery plans and procedures, including roles and responsibilities, communication protocols, and step-by-step instructions.

- [ ] Done
- [ ] In progress
- [ ] To-do

04

Regularly test and validate backup and recovery processes to ensure their effectiveness and identify any issues or gaps.

- [ ] Done/Process in place
- [ ] In progress
- [ ] To-do

05

Maintain an accurate inventory of backup data and systems, including their locations and recovery procedures.

- [ ] Done/Process in place
- [ ] In progress
- [ ] To-do

Incident Response Plan

An Incident Response Plan is a documented set of procedures that outline everything you need to do before, during, and after a cyber security incident. At Coretelligent, we follow the best practices in the SANS 6-Step Incident Response framework.

Key components of the SANS Incident Response framework include:

- **Preparation**
  Define roles and responsibilities, provide training, and ensure tools and resources are available to handle incidents effectively.
- **Identification**
  Monitor your infrastructure, detect compromise, and determine the scope and impact of the incident.
- **Containment**
  Immediately isolate affected systems, disable compromised user accounts, and prevent further damage.
- **Eradication**
  Remove the root cause of the incident (e.g., eliminating malware, patching vulnerabilities, etc.).
- **Recovery**
  Restore systems and data to their normal operating state and validate the incident has been fully resolved.
- **Lessons Learned**
  Review the incident and the effectiveness of your response to find ways to improve.

Timing Best Practice

Review and update incident response plans at least annually, as well as any time your IT infrastructure, processes, or regulatory requirements change significantly.

Why This Belongs in Your Cyber Security Toolkit

- ➜ Enables you to quickly detect and contain security incidents, minimizing their impact.
- ➜ Reduces security breach recovery time and associated costs.
- ➜ Protects your critical data integrity.
- ➜ Helps you maintain customer trust and confidence.
- ➜ Identifies areas to improve and strengthen your defense.

Incident Response Plan Checklist

01

Develop a comprehensive Incident Response Plan that outlines roles and responsibilities, communication protocols, and step-by-step procedures for a range of different scenarios.

- ☐ Done
- ☐ In progress
- ☐ To-do

02

Establish an Incident Response Team with clearly defined roles and responsibilities, and provide regular training and exercises.

- ☐ Done
- ☐ In progress
- ☐ To-do

03

Implement a Security Operations Center (SOC) or engage with an advanced IT services partner to provide 24/7 monitoring and incident response capabilities.

- ☐ Done
- ☐ In progress
- ☐ To-do

04

Regularly review and update your Incident Response Plan to ensure it aligns with your current infrastructure, processes, and regulatory requirements.

- ☐ Done/Process in place
- ☐ In progress
- ☐ To-do

05

Conduct periodic tabletop exercises and simulations to test the effectiveness of your Incident Response Plan and identify areas for improvement.

- ☐ Done/Process in place
- ☐ In progress
- ☐ To-do

TPRM / Vendor Management

Third-Party Risk Management (TPRM) or Vendor Management is the process of identifying, assessing, and mitigating risks associated with third-party vendors and service providers who have access to your critical data, systems, and IT infrastructure.

Key components of effective third-party risk management programs include:

- Up-to-date inventories of all third parties you work with, mapped to the data and systems they have access to.
- Due diligence assessments of third parties' cyber security postures, financial viabilities, business continuity plans, regulatory compliance status, and overall risk profile.
- Processes for ongoing third-party training, evaluation, and monitoring.
- Offboarding processes that revoke third-party access to systems and data, retrieve critical assets, and terminate contracts.

Timing Best Practice

Conduct third-party risk assessments prior to onboarding new vendors, and then annually, bi-annually, or whenever there are significant changes to vendors' services or responsibilities.

Why This Belongs in Your Cyber Security Toolkit

- ➜ Helps you meet third-party oversight requirements associated with regulations like GDPR, HIPAA, FISMA, and SOX.
- ➜ Provides a comprehensive view of all your third-party relationships.
- ➜ Enables you to proactively reduce risk exposure from your partner ecosystem.
- ➜ Ensures business continuity by monitoring and minimizing third-party risks to your critical operations.

Third-Party Risk Management Checklist

01

Develop a comprehensive third-party risk management program that spells out your processes for vendor risk assessments, due diligence, and ongoing monitoring.

- ☐ Done
- ☐ In progress
- ☐ To-do

02

Establish clear security requirements and expectations for vendors, including data protection, access controls, and incident reporting.

- ☐ Done
- ☐ In progress
- ☐ To-do

03

Implement contractual agreements and service level agreements (SLAs) to ensure vendor accountability and enforce security requirements.

- ☐ Done/Process in place
- ☐ In progress
- ☐ To-do

04

Regularly monitor vendor performance and compliance with regard to security requirements, and take appropriate actions to mitigate identified risks.

- ☐ Done/Process in place
- ☐ In progress
- ☐ To-do

Need help?

Explore our solutions and let us help check off your cyber security to-dos.

People

IT Steering Committee

- [ ] Technology Strategy & Planning
- [ ] Outsourced CISO Services

Security Awareness User Training

- [ ] Comprehensive Security Solutions & Training

Access Reviews

- [ ] Data & App Security Solutions

Technology

Mandatory MFA

- [ ] Cybersecurity & Compliance Solutions

Email Security

- [ ] Cybersecurity & Compliance Solutions

Endpoint Detection and Response (EDR)

- [ ] Cybersecurity & Compliance Solutions

Processes

Backup and Recovery

- [ ] Backup & Disaster Recovery Solutions

Incident Response Plan

- [ ] Outsourced CISO Services
- [ ] Cybersecurity & Compliance Solutions

TPRM / Vendor Management

- [ ] Outsourced CISO Services
- [ ] Cybersecurity & Compliance Solutions

coretelligent

Why Coretelligent?

We’re the business partner you can trust with every facet of your technology.

Our expertise is grounded in providing superlative managed IT support but also includes advanced capabilities in cyber security, compliance, data analytics, and workflow automation. From aligning your tech strategy to your business goals to planning and managing your cloud transformation, our engineers have the skills and experience you can count on.

→ Visit us online at Core.tech.