Devolutions

Cybersecurity vs IT security: Taking responsibility for organizational information security

NOVEMBER 2025

TABLE OF CONTENTS

For today's small and mid-sized businesses (SMBs), confidential data and corporate secrets sit at the center of everything: revenue generation, customer trust, and day-to-day operations. Sales records, financial transactions, intellectual property, and service delivery all depend on interconnected systems that are accessible from almost anywhere. **However, this unprecedented access and convenience has a cost: cybercrime.**

Recent research shows that despite their relatively smaller size, **SMBs are over-represented in global breach statistics.** One analysis found that companies with fewer than 250 employees accounted for 71% of data breaches in 2025. And the Devolutions State of IT Security in SMBs in 2024-2025 Survey report revealed that 43% of SMBs faced at least one cyberattack in the past year.

For SMBs, a serious cyberattack is not just an IT problem: it is a fundamental business problem with potentially catastrophic consequences. IBM's 2025 Cost of a Data Breach report pegs the average cost of a breach at $4.4 million USD per incident, and Microsoft estimates that cyberattacks cost SMBs more than 250,000 USD on average, and in some cases as much as a whopping $7 million once investigation, recovery, fines, and lost business are taken into account. And the story gets worse.

The threat landscape is continuously advancing and evolving. The latest analysis of Verizon's Data Breach Investigations Report shows that ransomware now features in 44% of breaches, which reflects attackers' focus on business disruption and extortion. And Microsoft's 2025 Digital Defense Report revealed that financially motivated cybercrime now dominates the threat landscape.

Yet despite these trends, many SMBs still underestimate and downplay their exposure. The Devolutions State of IT Security in SMBs in 2024-2025 Survey uncovered some alarming gaps:

- **80% of SMBs do not have a comprehensive plan for mitigating and managing insider threats.**
- **78% of SMBs do not have an advanced cybersecurity posture.**
- **52% of SMBs still manage privileged access using manual processes like spreadsheets, vaults, or no formal system at all.**

- **40% of SMBs aren't using AI at all to strengthen their cybersecurity profile.**
- **Only 39% of SMBs offer continuous cybersecurity training, and 17% offer none at all.**
- **29% of SMBs allocate less than 5% of their IT budget to IT security and cybersecurity.**

These worrisome statistics send a clear message: Limited budgets, small IT teams, and competing priorities make it extremely challenging for SMBs to respond with the same depth of defenses as large enterprises.

This is the context in which the terms cybersecurity and IT security are used. In reality, they describe related but distinct domains. Cybersecurity typically focuses on defending against active threats and adversaries, while IT security focuses on building and operating secure, resilient infrastructure and services. **For SMBs, understanding how these disciplines overlap and where they diverge is essential.** It affects who is accountable for what, how limited budgets are allocated, and how policies and controls are prioritized.

This white paper is designed to help SMBs eliminate the confusion and focus on practical responsibility for information security. Our roadmap covers:

- **Clear, business-focused definitions of cybersecurity and IT security.**
- **Where cybersecurity and IT security overlap.**
- **The key distinctions between the two disciplines, and why those differences matter for risk management, staffing, and budgeting**
- **The roles that typically carry responsibility for IT security and cybersecurity in an SMB, and how they support secure day-to-day operations**
- **Core elements of a strong IT security and cybersecurity policy and program.**
- **How IT security and cybersecurity can work together as a coordinated whole instead of separate efforts**

We wrap things up with a valuable discussion on how Devolutions solutions help SMBs establish and enforce both IT security and cybersecurity controls in a way that fits their size, complexity, and budget.

WHAT IS IT SECURITY?

IT security is the discipline that keeps an organization's technology environment dependable, controlled, and safe to operate. It focuses on protecting the IT assets that keep the business running: servers, endpoints, applications, networks, identities, and the data that flows through them. **Put simply, IT security is about making sure systems are configured correctly, access is appropriate, changes are controlled, and recovery is possible when things go wrong.**

While cybersecurity is often threat and adversary focused (as we explore in the next section), IT security is primarily operations focused. Its mandate is to ensure that:

- **Systems and services are available when the business needs them.**
- **Data remains accurate and complete as it moves and changes.**
- **Access to systems and data is limited to the right people, at the right time, for the right reasons.**
- **Technical environments are configured in line with policies, standards, and regulatory requirements.**

In practice, this mandate shows up in day-to-day work that many SMB IT teams already perform: patching servers, hardening configurations, maintaining backups, provisioning and deprovisioning accounts, and validating that systems keep working after changes.

WHAT IS CYBERSECURITY?

Cybersecurity is the discipline that protects an organization's digital assets from malicious activity. It focuses on defending systems, networks, applications, accounts, and data against attackers who are trying to steal information, disrupt operations, or gain unauthorized control. **Essentially, cybersecurity is the function that keeps a continuous eye on threats and ensures the organization is prepared to prevent, detect, and respond to them.**

While IT security is primarily rooted in operations, cybersecurity focuses on understanding threats, watching for attacks, and responding when something goes wrong. Its mandate is to ensure that:

- Exposure to external and internal attacks is identified, reduced, and continuously managed.
- Unauthorized access, misuse, and disruption are prevented wherever possible.
- Malicious activity is detected quickly across endpoints, networks, identities, and cloud services.
- Incidents are contained, investigated, and eradicated in a structured, repeatable way.
- Lessons from incidents, tests, and threat intelligence are used to improve controls and policies over time.

Examples of typical activities and tasks include: reviewing security alerts, tuning email and web filters to block phishing, investigating suspicious logins or privilege use, coordinating responses to malware or ransomware, updating security policies, and delivering or arranging cybersecurity awareness training.

In some SMBs, these tasks are handled by an internal security lead. In others, they are shared across the IT team, or delegated to a managed service provider. We explore various roles and responsibilities later in this white paper.

WHERE IT SECURITY AND CYBERSECURITY OVERLAP

Although IT security and cybersecurity emphasize different aspects of protecting the organization, there is significant overlap between them. Both disciplines exist to safeguard the same underlying assets: systems, data, users, and business processes. In addition, both support the same ultimate objectives: protect revenue, maintain customer trust, and keep operations running.

In an SMB, this overlap is especially visible. The same IT team or individual that patches servers and manages backups is often tasked with responding to phishing attacks, investigating suspicious logins, and reporting on security incidents. **The labels may differ, but the work frequently touches both IT security and cybersecurity at the same time.**

- **At a high level, IT security and cybersecurity align around several shared goals:**
- **Protecting sensitive data from unauthorized access, misuse, loss, or corruption.**
- **Maintaining the confidentiality, integrity, and availability of systems and services.**
- **Reducing the likelihood and impact of incidents that could disrupt operations.**
- **Meeting regulatory, contractual, and insurer expectations for information security.**
- **Demonstrating to customers and partners that the organization takes security seriously.**

They also rely on many of the same foundational controls. For example:

- **Identity and access management, including strong authentication and least privilege.**
- **Secure configuration and hardening of servers, endpoints, and network devices.**
- **Patch and vulnerability management across operating systems, applications, and firmware.**
- **Backup, recovery, and resilience practices that ensure critical data and services can be restored.**
- **Logging, monitoring, and alerting that provide visibility into what is happening across the environment.**
- **Security awareness and training that help users recognize and avoid common attack techniques.**
- **Governance through policies, standards, and procedures that define how technology is used and controlled.**

From an SMB perspective, the overlap is not a problem to be eliminated, but a reality to be leveraged. The same asset inventory can serve both IT security and cybersecurity. The same centralized access control strategy can support stable operations and reduce breach risk. And the same remote access platform can simplify administration and close dangerous exposure points.

Understanding this alignment helps SMBs avoid building separate, competing efforts. Instead, they can design controls, processes, and tools that serve both operational stability and threat defense at the same time.

WHERE IT SECURITY AND CYBERSECURITY DIFFER

As we just discussed, IT security and cybersecurity share many objectives. **However, they are not interchangeable.** Each discipline looks at the same environment through a different lens and focuses on different types of risk. For SMBs, understanding these distinctions is vital, because it influences how responsibilities are assigned, how tools are selected, and how limited budget is spent. At a high level, the key differences can be summarized as follows:

PRIMARY FOCUS

IT security is primarily focused on operations. It is concerned with building, configuring, and maintaining a technology environment and infrastructure that is stable, predictable, and safe to use. The central question is: «Are our systems, configurations, and processes set up correctly so people can do their jobs securely?»

Cybersecurity is primarily focused on threats. It concentrates on identifying, reducing, and responding to malicious activity. The central question is: «Are we prepared to prevent, detect, and respond to attackers who are trying to harm us?»

TIME HORIZON AND RHYTHM OF WORK

IT security tends to follow planned cycles and change windows. Activities are often scheduled and repeatable, such as monthly patching, quarterly access reviews, and regular backup tests.

Cybersecurity tends to involve more real-time or near real-time work. Teams must be able to respond quickly to alerts, investigate suspicious behavior, contain incidents, and adapt to new attack techniques as they appear.

MEASURES OF SUCCESS

Success in IT security is usually measured by:

- System uptime and service availability.
- Configuration compliance with policies and standards.
- Successful completion of backups and restores.
- Low rates of self-inflicted incidents and outages.

Success in cybersecurity is usually measured by:

- Number and severity of security incidents.
- Speed of detection, containment, and recovery.
- Reduction in successful phishing or credential theft.
- Coverage of monitoring across critical systems and identities.

TYPICAL ACTIVITIES AND DELIVERABLES

IT security activities often include:

- Provisioning and deprovisioning user accounts.
- Applying patches and configuration baselines.
- Managing remote access and network segmentation.
- Operating backup and recovery processes.
- Maintaining asset inventories and configuration records.

Cybersecurity activities often include:

- Reviewing and tuning security alerts and rules.
- Investigating suspicious logins, processes, or network traffic.
- Running incident response drills and refining playbooks.
- Managing security awareness training and phishing simulations.
- Consuming threat intelligence and adjusting defenses.

SKILLS AND TOOLS

IT security leans on skills related to system administration, networking, and infrastructure operations. Common tools include directory services, configuration management platforms, backup systems, virtualization platforms, and remote access tools.

Cybersecurity leans on skills related to threat analysis, incident response, and security engineering. Common tools include email and web security gateways, endpoint detection and response, security information and event management (SIEM), and specialized incident management platforms.

STAKEHOLDERS AND COMMUNICATION

IT security typically communicates in terms of systems, configurations, and service levels. The primary stakeholders are IT leadership, line-of-business owners who depend on availability, and vendors or MSPs that help keep systems running.

Cybersecurity typically communicates in terms of risk, threats, and incidents. The primary stakeholders are executives, risk and compliance owners, insurers, and in some cases regulators and customers who want assurance that their data is protected.

For SMBs, these various distinctions do not mean that separate teams are always required. In many organizations, the same people perform both IT security and cybersecurity tasks. However, recognizing where the disciplines differ helps clarify expectations. **It makes it easier to assign ownership, prioritize investments, and ensure that both the operational foundation and the threat response capability receive the attention they need.**

WHO IS RESPONSIBLE FOR IT SECURITY?

In most SMBs, IT security is not owned by a large, specialized team. As mentioned a moment ago, it is usually carried by a small group of IT professionals (sometimes supported by external partners). Understanding who does what is essential for closing gaps, avoiding duplicate effort, and making sure that key responsibilities do not fall through the cracks. At a high level, IT security in an SMB typically involves the following roles.

IT LEADERSHIP

Titles may include IT manager, head of IT, IT director, or similar. In many SMBs, this is a single person. Their responsibilities usually include:

- Setting the overall strategy for the IT environment and aligning it with business priorities.
- Approving IT security policies and standards, and ensuring they are realistic for the organization.
- Selecting key platforms and vendors that affect IT security posture.
- Owning the IT budget, including investments in security tooling and training.
- Reporting risks, issues, and major incidents to senior leadership.

SYSTEM AND NETWORK ADMINISTRATORS

These are the hands-on operators who build and maintain the core infrastructure. They often hold titles like systems administrator, network administrator, or infrastructure specialist. Their responsibilities typically include:

- Provisioning and deprovisioning user accounts and groups.
- Applying patches and configuration baselines to servers, endpoints, and network devices.
- Managing directory services, VPNs, firewalls, and remote access platforms.
- Implementing backup and recovery processes, and testing restores.

- Hardening systems in line with policies, checklists, and best practices.
- Troubleshooting issues in a way that preserves security controls instead of working around them.

SERVICE DESK AND SUPPORT STAFF

Front-line support teams play a critical role in IT security. Their responsibilities often include:

- Enforcing identity verification procedures before resetting passwords or changing access.
- Escalating suspicious behavior, such as unusual access requests or repeated lockouts.
- Educating users informally about secure practices during support interactions.
- Logging and categorizing incidents that have a security component.
- Applying standard fixes that are designed to be secure by default.

CLOUD AND SAAS ADMINISTRATORS

As SMBs move core services into the cloud, specialized administrators or technically inclined business owners often become responsible for individual platforms, CRM systems, and line-of-business applications. Their responsibilities usually include:

- Configuring tenant level security options and secure defaults.
- Managing roles, licenses, and application specific permissions.
- Enabling multifactor authentication and conditional access where available.
- Controlling external sharing, data export, and integration settings.
- Coordinating with IT to ensure that cloud configuration aligns with internal policies.

APPLICATION AND DATA OWNERS

These are not always IT roles. They can be finance managers, operations leaders, or other business owners who are responsible for critical applications and the data they contain. Their responsibilities often include:

- Defining who should have access to specific applications and datasets.
- Approving access requests and periodic access reviews.
- Working with IT to classify data and set appropriate protection levels.
- Participating in backup, recovery, and business continuity planning for their systems.

MANAGED SERVICE PROVIDERS (MSPS) AND EXTERNAL PARTNERS

Some SMBs augment their small internal team with an MSP or other IT partners. These providers may deliver some or all of the day-to-day IT security operations. Their responsibilities typically include:

- Monitoring and maintaining infrastructure, endpoints, and core services.
- Applying patches and updates according to agreed schedules.
- Managing and monitoring backup jobs, and assisting with restores.
- Providing recommendations on configuration, hardening, and new controls.
- Escalating significant issues and helping coordinate response when incidents occur.

In practice, these roles are often combined. An IT manager may also act as system administrator. A power user in finance may effectively be the data owner and application administrator for the accounting system. An MSP may handle both remote access and backup management. **What matters is not the title, but the clarity of responsibility.**

For IT security to be effective in an SMB, each of these areas needs a clearly identified owner, a basic set of documented expectations, and a way to coordinate with others. This creates the foundation on which more advanced cybersecurity capabilities can be built.

WHO IS RESPONSIBLE FOR CYBERSECURITY?

Similar to IT security, in SMBs cybersecurity is not handled by a large, dedicated security operations center. Instead, it is shared across a mix of internal staff (and possibly external partners) who watch for threats, respond to incidents, and guide overall security strategy. Understanding these roles helps SMBs avoid blind spots and make sure that real attackers do not slip through the cracks simply because "no one owned it." At a high level, cybersecurity in an SMB typically involves the following roles.

SECURITY LEADERSHIP (CISO, SECURITY LEAD, OR SECURITY CHAMPION)

In SMBs, this role is often owned by an IT leader, technical founder, or appointed "security champion." Responsibilities usually include:

- Owning the overall cybersecurity strategy and roadmap.
- Performing or coordinating risk assessments and prioritizing controls.
- Approving cybersecurity policies and standards.
- Aligning cybersecurity efforts with business priorities, contracts, and regulatory obligations.
- Reporting meaningful security risks and incidents to executive leadership and the board.

SECURITY OPERATIONS AND ANALYSIS

These responsibilities may be handled by an internal security analyst, by IT staff with a security focus, or by an external managed security service provider. Typical responsibilities include:

- Monitoring alerts from security tools such as email security, endpoint protection, and identity platforms.
- Investigating suspicious logins, endpoint activity, or network traffic.
- Tuning detection rules and security policies to reduce noise and improve coverage.
- Coordinating containment steps, such as blocking accounts or isolating devices.

- Documenting findings and recommending improvements to controls and configurations.

INCIDENT RESPONSE COORDINATOR

In the immediate aftermath of a serious incident, someone must step up and take charge. In SMBs this is often the IT manager, security lead, or an external specialist. Responsibilities usually include:

- Activating the incident response plan and assigning roles.
- Ensuring that evidence is preserved for investigation and potential legal or insurance needs.
- Coordinating communication with executives, affected business units, and external parties.
- Working with technical staff and providers to contain, eradicate, and recover from the incident.
- Leading or commissioning post-incident reviews and tracking follow-up actions.

GOVERNANCE, RISK, AND COMPLIANCE (GRC) OWNER

This role may sit in IT, finance, operations, or a general management function. The focus is on structure and accountability rather than day-to-day technical work. Responsibilities often include:

- Maintaining the security policy set and ensuring it is reviewed regularly.
- Managing the risk register and tracking mitigation plans.
- Coordinating responses to security questionnaires from customers, partners, and insurers.
- Owning documentation needed for audits, certifications, and regulatory obligations.
- Ensuring that cybersecurity requirements are reflected in vendor and customer contracts.

Awareness and training owner

Users remain a primary target for attackers, so someone must own the "human side" of cybersecurity. In SMBs this might be HR, an IT manager, or a security champion. Responsibilities usually include:

- Selecting and coordinating cybersecurity awareness training programs.
- Running or arranging phishing simulations and follow-up education.
- Ensuring that new hires receive basic security onboarding.
- Tailoring training for high-risk roles such as executives, finance, and administrators.
- Reinforcing secure behavior through internal communications and reminders.

MANAGED SECURITY SERVICE PROVIDERS (MSSPS, MDR PROVIDERS, AND OTHER EXTERNAL PARTNERS)

Since SMBs rarely have the budget or need for a full-time security team, external providers often carry a significant portion of the cybersecurity workload. Depending on the service level agreement, their responsibilities can include:

- Providing and operating tools such as endpoint detection and response, SIEM, and email security.
- Monitoring environments for indicators of compromise and suspicious behavior.
- Investigating alerts and providing clear, actionable guidance when risk is identified.
- Assisting with incident response and forensics during serious events.
- Advising on improvements to security architecture, policies, and controls.

In practice, these roles frequently overlap and are combined. An IT manager may act as both security lead and incident coordinator. A single MSP may provide general IT support as well as managed detection and response services. A finance director may double as the risk and compliance owner.

As with IT security, what matters most is not the job title but the clarity of responsibility. Every SMB should be able to answer questions such as: Who owns our cybersecurity strategy? Who is watching for attacks right now? Who leads if we have a serious incident tomorrow? When these answers are clear, it becomes much easier to build a cybersecurity function that complements IT security and provides real protection against modern threats.

CORE ELEMENTS OF A STRONG IT SECURITY POLICY AND PROGRAM

A strong IT security program gives SMBs structure, consistency, and a shared understanding of how technology should be built and operated. It turns good intentions into clear expectations and repeatable practices. For most organizations, the core elements fall into four areas: governance, configuration, identity, and resilience.

GOVERNANCE AND ACCOUNTABILITY

Governance defines how decisions are made, who is responsible for what, and which rules apply across the IT environment. Without it, even good technical work can become inconsistent and fragile. A solid governance foundation for IT security typically includes:

- **Documented policies and standards:** Clear, concise documents that explain how systems must be configured, how access is granted, how remote work should be handled, and how data must be protected. Policies do not need to be long, but they must be understandable and accessible.
- **Defined roles and responsibilities:** Clarity about which roles own which parts of IT security. For example, who approves changes to firewall rules, who decides when to grant admin access, who owns backup strategy, and who is accountable for vendor risk.
- **Change management:** A simple but consistent process for planning, reviewing, and approving changes that affect security. This can be as lightweight as a shared calendar and a checklist, as long as it prevents untracked, high-risk changes.
- **Vendor and SaaS oversight:** Expectations for how external providers are selected, onboarded, and reviewed, particularly when they handle critical systems or data. This includes documenting which providers have administrative or remote access.

Governance does not have to be complex or bureaucratic. The goal is to make sure that important decisions are intentional, documented, and owned by specific people or teams.

CONFIGURATION AND ASSET MANAGEMENT

IT security depends on knowing what you have and how it is configured. If assets and settings are unknown or unmanaged, it becomes almost impossible to control risk. Key elements in this area include:

- **Asset inventory:** A current list of servers, endpoints, network devices, cloud services, and critical applications. This inventory should include owners, locations, and basic details such as operating system and purpose.
- **Standard configurations and baselines:** Agreed settings for new systems, such as required security controls, encryption, logging, and local account policies. Using standard images or templates reduces the chance that important controls are missed.
- **Patch and update management:** A structured approach for applying operating system, application, and firmware updates. This typically includes regular cycles, emergency patching procedures, and basic testing for critical systems.
- **Configuration tracking:** The ability to see what has changed over time, at least for key systems. This might be through configuration management tools, scripts, or stored export files, as long as IT can answer the question: «What changed before this problem appeared?»

When configuration and asset management are handled well, the environment becomes more predictable and easier to secure.

IDENTITY AND ACCESS MANAGEMENT

Identity and access are at the center of both IT security and cybersecurity. For IT security, the focus is on making sure that the right people have the right level of access, and that privileged capabilities are tightly controlled. Core elements of identity and access management in an IT security program can include:

- **Account lifecycle processes:** Standard procedures for creating, modifying, and disabling accounts when people join, move within, or leave the organization. This should cover employees, contractors, vendors, and service accounts.
- **Role-based access and least privilege:** Access rights based on job roles rather than one-off, individual decisions. The default should be the minimum access required to perform the job, with privileged access granted only when clearly justified.

- **Privileged account management:** Extra safeguards for administrator accounts and high-impact permissions, including unique credentials, strong authentication, and reduced day-to-day use. Shared admin passwords and unmanaged service accounts significantly increase risk.
- **Authentication standards:** Requirements for password length and complexity, multifactor authentication for sensitive systems, and secure handling of authentication tokens.
- **Regular access reviews:** Periodic checks with business owners and application owners to confirm that users still need the access they have, particularly for high-risk systems and roles.

When identity and access management is structured and enforced, it becomes much harder for simple mistakes or outdated permissions to turn into serious incidents.

RESILIENCE: BACKUP, RECOVERY, AND CONTINUITY

Even with strong controls, incidents and failures can occur. Resilience is about making sure the business can recover. In IT security, that means thinking beyond individual systems and considering how quickly critical services and data can be restored. Important elements of resilience include:

- **Backup strategy:** Clear decisions about what is backed up, how often, where backups are stored, and how long they are retained. This should cover servers, key applications, configuration data, and any other information that would be costly or impossible to recreate.
- **Segregation and protection of backups:** Measures to ensure that backups are not easily corrupted, deleted, or encrypted by the same incident that affects production systems. This can involve offline copies, immutable storage options, or logically separate backup accounts and locations.
- **Restore testing:** Regular, documented tests that prove systems and data can be restored successfully within acceptable timeframes. A backup that has never been tested is a risk, not a guarantee.

- **Basic continuity planning:** Identification of the most critical systems and processes, along with simple plans for how the organization will operate during outages and recoveries. This does not need to be a complex business continuity framework, but it should answer practical questions such as «What do we do if our main file server is unavailable for two days?»

Resilience is where IT security has a direct, visible impact on the business. Effective backup and recovery work can turn a serious incident into a manageable interruption rather than a long-term crisis.

BRINGING THE ELEMENTS TOGETHER

Governance, configuration, identity, and resilience are tightly linked. Governance defines expectations. Configuration and asset management make the environment knowable and consistent. Identity and access management control who can do what. Resilience ensures that the organization can recover when things go wrong.

For SMBs, the goal is not perfection in each of these areas. It is to establish clear, workable practices that can be maintained by a small team and adapted as the business grows.

In the next section, we will look at how a strong cybersecurity policy and program builds on this IT security foundation to address active threats and adversaries.

CORE ELEMENTS OF A STRONG CYBERSECURITY POLICY AND PROGRAM

A strong cybersecurity program gives SMBs a structured way to understand threats, reduce exposure, and respond when attacks occur. It complements IT security by focusing on adversaries and attack paths rather than on systems and configurations. At a practical level, a strong cybersecurity program is built around three pillars: threat prevention, detection, and incident response, all guided by clear policy and governance.

STRATEGY, RISK, AND GOVERNANCE

Cybersecurity cannot be effective if it consists only of tools and alerts. It needs direction. Strategy, risk, and governance provide that direction and keep efforts aligned with business priorities. Key elements include:

- **Defined cybersecurity objectives:** Clear statements of what the organization is trying to achieve, such as reducing ransomware risk, protecting customer data, or meeting specific contractual requirements.
- **Risk assessment and prioritization:** Regular, lightweight reviews of key risks, focusing on the systems and processes that would hurt the business most if they were compromised. This helps SMBs concentrate limited resources on what matters most.
- **Documented cybersecurity policies:** Policies that describe how the organization handles topics such as acceptable use, remote work, third-party access, data classification, and password standards. These should align with and extend the IT security policies already in place.
- **Assignment of ownership:** Clear identification of who owns cybersecurity strategy, who manages day-to-day defense, and who leads during incidents. Ownership is especially important in SMBs where people wear multiple hats.

THREAT PREVENTION

Threat prevention reduces the number of successful attacks that ever reach critical systems or users. It focuses on closing common entry points and making it harder for attackers to gain a foothold. Core preventive elements include:

- **Email and web security controls:** Filters that block known malicious attachments, links, and domains, and that help identify phishing attempts. For many SMBs, this is the first line of defense against socially engineered attacks.
- **Secure identity and access practices:** Multifactor authentication for remote access, admin accounts, and key cloud services, combined with strong password policies and controls that limit lateral movement if credentials are compromised.
- **Baseline hardening of endpoints and servers:** Configuration standards that reduce exploitable weaknesses, such as disabling unnecessary services, restricting macro execution where possible, and limiting local administrator rights.

- **Application and cloud security settings:** Use of built-in security features in SaaS and cloud platforms, such as conditional access, session controls, and suspicious activity alerts. Ensuring that default settings are reviewed and tightened where needed.
- **Awareness and behavior change:** Continuous, practical cybersecurity training that helps users recognize phishing, social engineering, and risky behavior. The goal is to reduce the likelihood that human error will open the door to attackers.

Prevention will never be perfect, but consistent work in these areas significantly lowers the volume and impact of attacks that reach the environment.

DETECTION AND VISIBILITY

Even with strong prevention, some attacks will succeed or partially succeed. Detection and visibility focus on spotting malicious activity quickly, before it turns into a major breach. Key elements include:

- **Centralized logging of critical systems:** Collection of logs from identity platforms, email systems, endpoints, servers, and key applications. Logs must be reliable and readily available when there is something to investigate.
- **Security monitoring and alerting:** Use of security tools that can generate meaningful alerts on suspicious activity, such as unusual login patterns, privilege escalations, malware detections, or unexpected changes to critical configurations.
- **Defined alert handling processes:** Simple workflows that describe who reviews alerts, how quickly they are expected to respond, and how alerts are escalated if they appear serious. This can be handled internally or through a managed security provider.
- **Use of threat intelligence and built-in security insights:** Leveraging threat feeds and vendor insights that can highlight emerging attack techniques, new malicious domains, or campaigns that target specific industries or regions.

Effective detection does not require a full-scale security operations center. For SMBs, the priority is to ensure that someone is watching the most important signals, and that there is a clear plan for what to do when those signals indicate trouble.

INCIDENT RESPONSE AND RECOVERY

Incident response is the capability that turns potential chaos into a structured process. It defines how the organization reacts when it suspects or confirms that an attack is in progress or has already occurred. Core elements include:

- **Incident response plan:** A concise, practical document that outlines roles, communication paths, decision points, and basic steps for investigation, containment, eradication, and recovery. The plan should be understandable by people who are not security specialists.
- **Playbooks for common incident types:** Step-by-step guides for handling likely scenarios such as phishing, credential theft, malware infection, or suspected data exfiltration. These playbooks can be short checklists, as long as they are realistic and tested.
- **Clear communication channels:** Defined methods for informing executives, affected employees, external partners, and in some cases customers or regulators. This includes guidance on what can be shared when facts are still emerging.
- **Coordination with IT security and business continuity:** Alignment with backup, recovery, and continuity plans so that technical actions taken during an incident do not inadvertently cause extended downtime or data loss.
- **Post-incident reviews:** Structured reviews that capture what happened, what worked, what did not, and which improvements are needed. The goal is to ensure that each incident results in a stronger posture, not just a return to the previous state.

CONTINUOUS IMPROVEMENT AND CULTURE

Cybersecurity is not a one-time project. Threats evolve, systems change, and attackers look for the easiest available targets. For this reason, continuous improvement and culture are essential parts of a strong cybersecurity program. Key elements include:

- **Regular review cycles:** Periodic checks of policies, controls, and risk assessments to ensure they remain aligned with the current environment and threat landscape.
- **Metrics and reporting:** Simple measures that help leadership understand progress, such as phishing failure rates, time to respond to high-severity alerts, or the percentage of critical systems covered by multifactor authentication.

- **Security built into projects and procurement:** Including basic security questions and requirements when evaluating new systems, services, or vendors, rather than trying to retrofit controls later.
- **Reinforcement of secure behavior:** Ongoing communication that treats security as a shared responsibility. Recognizing good practices, rather than only focusing on mistakes, helps sustain engagement.

When these core elements are in place, cybersecurity becomes a structured, predictable part of how the organization operates. It pairs with IT security to provide both a hardened environment and a focused capability to prevent, detect, and respond to real-world attacks.

HOW IT SECURITY AND CYBERSECURITY CAN WORK TOGETHER AS A COORDINATED WHOLE

IT security and cybersecurity are often described as separate disciplines, but in an SMB they share the same reality. The same lean team typically manages user accounts, applies patches, responds to phishing emails, restores backups, and explains incidents to leadership. Treating IT security and cybersecurity as completely separate efforts can lead to duplicated tools, conflicting priorities, and gaps in coverage. **Treating them as a coordinated whole helps SMBs get more value from every control, process, and hour of effort.**

At a practical level, IT security provides the foundation and cybersecurity builds on top of it. Strong configuration standards, disciplined change management, reliable backups, and clear access controls make it easier to prevent and contain attacks. In turn, cybersecurity insights highlight where IT security needs to be strengthened. For example, repeated account compromises may point to weak authentication, and recurring malware infections may reveal gaps in endpoint hardening or software management.

There are several areas where coordination makes a significant difference for SMBs:

- **Shared governance and ownership:** Use a single, integrated set of policies that covers both IT security and cybersecurity, rather than separate documents that drift out of sync. Clearly name the roles that own each policy, and ensure that the same people are involved when decisions affect both operations and risk.

- **Common inventories and architecture:** Maintain one source of truth for assets, identities, and critical applications. IT security uses this to manage configurations and patching. Cybersecurity uses it to understand attack paths, prioritize monitoring, and identify high value targets.
- **Aligned controls and tools:** Favor tools and platforms that serve both disciplines at once. For example, a central remote access solution can support secure administration, enforce least privilege, and provide session logging for investigations. A well configured identity platform can simplify user onboarding, while also enforcing multifactor authentication and conditional access.
- **Integrated monitoring and response:** Ensure that operational alerts and security alerts inform each other. Performance or availability issues may be early signs of an attack. Security detections may reveal misconfigurations or failing hardware. When IT security and cybersecurity review these signals together, they can respond more quickly and with better context.
- **Joint planning and prioritization:** When planning upgrades and projects, evaluate them from both perspectives. A planned network refresh is also an opportunity to improve segmentation. A move to a new SaaS platform is also a chance to standardize identity integration and strengthen access controls. This avoids "security as an afterthought" and reduces rework.

Yet again, we repeat the central message because it is so important to understand: In many SMBs, the same people already wear both IT and security hats. **The goal is not to create extra layers of process, but to make the dual role explicit.** When IT security and cybersecurity are treated as two parts of the same information security function, it becomes easier to coordinate work, explain priorities to leadership, and show how each investment supports both stable operations and meaningful risk reduction.

This coordinated approach also sets the stage for more effective use of tools and partners. Platforms that centralize access and enforce policy can support both IT security and cybersecurity goals at the same time, and external providers can plug into a clear structure rather than a collection of disconnected tasks.

HOW DEVOLUTIONS HELPS SMBS OPERATIONALIZE IT SECURITY AND CYBERSECURITY

Devolutions provides an integrated, SMB-focused platform for remote connection management, credential and secrets vaulting, and privileged access management. The solutions are designed to centralize access, enforce policy, and provide audit-ready evidence, while remaining fast to deploy and affordable for small IT teams.

In practical terms, Devolutions helps SMBs bring IT security and cybersecurity together through:

- **Stronger IT operations and remote access:** Remote Desktop Manager helps SMBs centralize remote sessions, manage privileged credentials, configure secure remote access, and restrict permissions to specific users.
- **Governed credential vaulting and PAM:** Devolutions Server (on-premises) and Devolutions Hub Business (cloud-based) provide shared, governed vaults for workforce and privileged credentials, with role-based access and auditing. Devolutions PAM builds on this to offer IT-led privileged access management that is enterprise-grade, but simplified and priced for SMBs and supports key functions such as account discovery, rotation, and approval-based access.
- **Reduced remote access and session risk:** Devolutions Gateway creates a secure entry point for segmented networks that require authorized just-in-time access, and works with Remote Desktop Manager to broker and record remote sessions without exposing internal services directly to the internet.
- **Audit, compliance, and continuous improvement:** Centralized logging, session recording, and detailed activity traces support investigations, insurer and auditor requests, and various compliance frameworks.

Together, these capabilities allow SMBs to implement practical controls for both IT security and cybersecurity, using tools that match their size, complexity, and budget.

NEXT STEPS

Ready to turn the knowledge in this white paper into concrete controls? Devolutions offers several risk-free and no-cost ways to get started, evaluate fit, and build internal consensus:

- **Request a free trial:** A trial key gives you access to the full Devolutions platform, so you can explore solutions such as Remote Desktop Manager, Devolutions Hub, Devolutions Server, Devolutions PAM, and Devolutions Gateway in your own environment.
- **Book a live guided demo:** Schedule a session with a Devolutions specialist to go deep into various solutions, and assess relevance and fit for your specific challenges, use cases, and objectives.
- **Run a proof of concept:** For an even deeper validation, request a structured, guided proof of concept to test workflows, policies, and integrations with real use cases. Only a minimal time investment is required on your part, and the engagement typically lasts 30-90 days.

All of these options empower you to move from theory to practice at your own pace. You can validate how Devolutions supports both IT security and cybersecurity requirements, and confirm that the approach fits your size, complexity, and budget, before rolling out more broadly.