

■ A PRACTICAL GUIDE

Technology & Security Improvements

Find the RUST. Build what will PASS.

ALEXANDRA DENSMORE
/ ELEVATE SERVICES GROUP

RUST

Find the weak point.

R

Risk

What is the business consequence if it fails or is misused?

U

Uptime

Is it doing its job, and doing it effectively?

S

Support

Who fixes it? How often does it need to be fixed?

T

Timeline

When do review and replacement (EOL) happen?

PASS

Test the proposed fix.

P

Productive

Does it remove a real delay, repeated task, or handoff?

A

Available

Does it keep work moving or shorten recovery?

S

Simple

Does it reduce systems, dependencies, or special knowledge?

S

Secure

Does it reduce unauthorized access, fraud, or exposure?

Good technology aligns to five operating outcomes.

01	SECURITY	Protect people, money, systems, and information.
02	CONTINUITY	Keep essential work moving. Systems and users are always available and perform optimally.
03	PRODUCTIVITY	Promote the successful outcomes of your business.
04	MANAGEMENT	Accurately predict how users and systems behave.
05	CENTRALIZATION	Keep data and controls with the company. Consolidate, leverage, and simplify systems and data.

Security: be in command of your business data and costs.

PURPOSE

Make your systems trustworthy, supportable, and recoverable.

There is an assumed trust from your customers and partners that you are secure. Losing customer trust from a security event is much more expensive than protecting it in the first place.

HIDDEN DEPENDENCY

Personal accounts, unapproved apps (Shadow IT & Shadow AI), shared access, and workarounds the company cannot see (and could unknowingly be paying for).

PRACTICAL MOVE

Make the secure path the easiest: approved tools, simple access, short training, and a clear request path. Ensure your cybersecurity program has modern protection layers.

Potential: implement a SaaS management platform and 3rd-party SOC.

ASK

Where is work happening outside company-approved accounts, apps, or systems?

ALIGNS TO

SECURITY

CONTINUITY

PRODUCTIVITY

MANAGEMENT

CENTRALIZATION

Threat Landscape Snapshot

27.7%

Manufacturing was IBM X-Force's most-targeted industry in 2025, representing 27.7% of observed incidents. That is the fifth consecutive year it ranked first.

The most targeted sector.

\$3.046B

in reported 2025 business email compromise losses across 24,768 complaints.

About \$123,000 per reported complaint.

Practical response:

strong identity, payment call-backs, known ownership, network boundaries, and tested recovery.

It is **imperative** that your Cybersecurity Program include modern and intelligent protection layers.

- **Zero Trust Identity & Access Management (IAM):** verify every user and device, grant only the access each role needs
- **Attack Surface Command:** every app, account, and AI tool touching your data is known and controlled
- **Continuous Vulnerability Management:** scan, prioritize, and patch weaknesses before attackers exploit them
- **Managed Detection & Response (MDR):** a 24/7 SOC that detects, investigates, and contains threats in real time
- **Cyber Resilience & Recovery:** tested backups and incident response that restore operations fast
- **AI-Driven Security Operations:** automation and analytics that widen coverage without adding headcount
- **Established Governance Framework :** maintain policies and procedures in a central repository - conduct regular reviews, staff trainings, and require staff and vendor attestations.

Phones: keep the customer path with the company.

PURPOSE

Keep calls, texts, photos, and routing available to the business.

HIDDEN DEPENDENCY

The main number, customer history, or routing lives with one person or one building.

PRACTICAL MOVE

Cloud-based company-controlled calling and texting.

Potential: it integrates into CRM/ERP. You can text or call from the mobile app, creating agility.

ASK

If this building went dark at 10:00 a.m., where would the next customer call or text go?

ALIGNS TO

SECURITY

CONTINUITY

PRODUCTIVITY

MANAGEMENT

CENTRALIZATION

Cameras: deliver evidence, not just live video.

PURPOSE

Usable evidence for claims, theft, safety incidents, liability, and access disputes.

HIDDEN DEPENDENCY

No one owns retention, camera logins, uptime, or how to pull footage when it's needed.

PRACTICAL MOVE

Spec replacements on resolution, low-light range, retention, and a tested export path.

Potential: tie-in to door badges, Entra, and remote access via cloud from anywhere on an approved device.

ASK

If an incident happened last week, could we easily pull clear footage of it?

ALIGNS TO

SECURITY

CONTINUITY

PRODUCTIVITY

MANAGEMENT

CENTRALIZATION

Website: keep the front door under company control.

PURPOSE

Establish credibility, answer basics, and route inquiries to an accountable owner.

HIDDEN DEPENDENCY

Domain, DNS, hosting, or renewals live in an employee or agency account.

PRACTICAL MOVE

Company-owned accounts, auto-renewal, MFA, and tested routing.

Potential: add a website assistant that guides a visitor to the most relevant information (example: navu.co).

ASK

If the designer or developer disappeared tomorrow, could we update the site and keep it secure?

ALIGNS TO

SECURITY

CONTINUITY

PRODUCTIVITY

MANAGEMENT

CENTRALIZATION

Payments: centralize the process, separate the decision.

PURPOSE

Invoice, receive, approve, and reconcile money with less delay and lower risk of fraud.

HIDDEN DEPENDENCY

A banking change is accepted inside one email thread without independent verification.

PRACTICAL MOVE

Controlled portal, role separation, and call-back verification using a known number.

Potential: make ACH the default for stronger financial predictability.

ASK

What happens before staff act on a convincing request to change banking details?

ALIGNS TO

SECURITY

CONTINUITY

PRODUCTIVITY

MANAGEMENT

CENTRALIZATION

AI readiness starts with operational readiness.

01

THE WORK

What manual or time-consuming task, or information problem should improve?

02

THE DATA

What company information will the tool see, and does the company securely control it?

03

THE REVIEW

Who verifies the result before it affects a customer, payment, quality, or production?

AI can prepare, summarize, organize, and communicate.
A person still owns the decision.

Fix what creates value first.

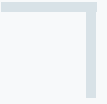
- 01 Revenue or cash interruption

- 02 Safety, quality, or dispute exposure

- 03 No workable manual fallback

- 04 One person, account, or device for a core system or process

- 05 Known support, renewal, or replacement deadline



■ STRATEGIC LENS

How does this *drive*
the *value chain* of the business?

Five questions:

- 01 Does it reduce costs, delays, rework, or risk?

- 02 Does it improve quality, speed, visibility, or decision-making?

- 03 Does it enable a new product, service, revenue stream, or business model?

- 04 Does it strengthen differentiation, customer loyalty, compliance, or resilience?

- 05 Can the impact be measured through KPIs such as margin, time to deliver, customer satisfaction, error rate, revenue, or risk exposure?
