FERRARA IT

National Self-Help Housing Conference

Risk Management

ABOUT FERRARA IT

FERRARA IT

Ferrara IT is a Managed IT Services Provider (MSP) and Managed Security Services Provider (MSSP) dedicated to delivering cutting-edge IT solutions for businesses that demand reliability, security, and compliance.

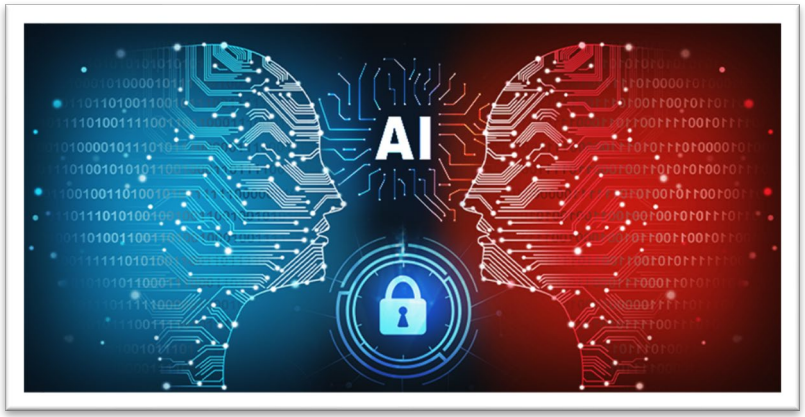
With a security-first approach, we provide comprehensive IT management, cybersecurity, cloud solutions, compliance services, and strategic IT consulting tailored to meet the needs of growing organizations.

THE REALITY OF CYBERSECURITY RISKS

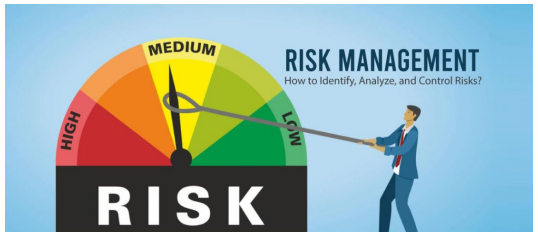
- The **threat landscape has changed**: It's not just about doing the right things in IT security anymore.
- Advancements in AI and the rise of cybercrime are creating new and **evolving risks**.
- **All businesses**, big or small, are **at risk**.
- We'll discuss key concepts to protect against data breaches.

CYBERSECURITY TODAY: WHAT HAS CHANGED?

- The era of preventing breaches with traditional IT practices is over.
- New **cyber threats leverage AI** and more sophisticated tactics.
- **Cybercriminals** are getting **more sophisticated**, and all businesses are now targets.



IDENTIFYING YOUR ORGANIZATION'S RISKS



Risk Factors: Data loss, downtime, reputational damage, and financial costs.

Perform an Information Asset Inventory:

- What types of sensitive data do you have (e.g., PII, HIPAA, contractual compliance)?
- Where is this data located?
- Who has access to it?
- Sensitive Data Protection: Understanding the value and risks of your data.

DATA ACCESS CONTROL

Limiting Exposure with Least Privilege Access

- Grant access only to individuals who **absolutely need it**.
- This reduces the chance of data theft or accidental exposure. *Example*: Even trusted employees should only have access to the data they need for their job.
- **Non-IT personnel should not** have local PC **admin access** to prevent unnecessary risks and potential exposure.
- Mitigate risks through controlled access.

EVALUATING THE IMPACT OF A CYBERSECURITY INCIDENT

What Happens When Things Go Wrong?

- The average dwell time for a breach is over 250 days (time from infection to remediation).
- Understand the business impact: Data loss, financial, operational disruption, and reputation.
- Evaluate your organization’s tolerance for risk and potential costs.

RISK MANAGEMENT: THE PLAN

Building a Strong Security Framework

- Written Information Security Program (WISP): Document policies, procedures, and response strategies.
- Roles & Responsibilities: Set clear expectations before a crisis.
- Controls: Use Antivirus, EDR, monitoring tools, policies, and training.

Operational Resilience

- Risk Analysis: Identify vulnerabilities beyond IT.
- Contingency Planning: Prepare for office inaccessibility or system failures.

PLANNING FOR CYBERSECURITY BREACHES

Expect the Unexpected: Plan for Breaches

- It’s impractical to think your organization will never be breached.
- Shift focus from prevention to detection, isolation, remediation.
- Limit the impact of a breach by responding quickly.

A MULTI-LAYERED APPROACH TO RISK MANAGEMENT

Prevention: Technical controls, antivirus, firewalls (and many more)

Detection: Continuous monitoring and anomaly detection. Example: SIEM (Security Information and Event Management).

Response:

- Endpoint Detection and Response (EDR) solutions.
- Managed Detection and Response (MDR) services.

Training: Equip your employees to recognize phishing, scams, etc.

Backups: Test and verify your backup procedures regularly.

Insurance: Get appropriate amounts of cyber coverage and consider overestimating your needs until the costs become untenable or coverage amounts are excessive.

CYBER INSURANCE: AN ESSENTIAL COMPONENT OF RISK MANAGEMENT

- Consider **cyber insurance** as part of your **risk mitigation** plan.
- Insurance companies are risk-averse: The more **mature your security practices**, the **lower your premiums**.
- Make sure you understand the policy, fill out the questionnaire correctly, and have someone guide you through the process.
- Cyber insurance does not replace good cybersecurity practices but provides a **safety net in case of failure**.

PUTTING IT ALL TOGETHER: BE PREPARED, BE PROTECTED

Act now: Start with an information asset inventory and risk assessment.

Invest wisely: Cybersecurity, insurance, and employee training.

Create a plan: Prepare for a breach even if you hope it never happens.

Partner with experts: Consult with IT professionals and insurance brokers to optimize your strategy.

FERRARA IT

Want to Learn More?

Email us at: Info@FerraraIT.com