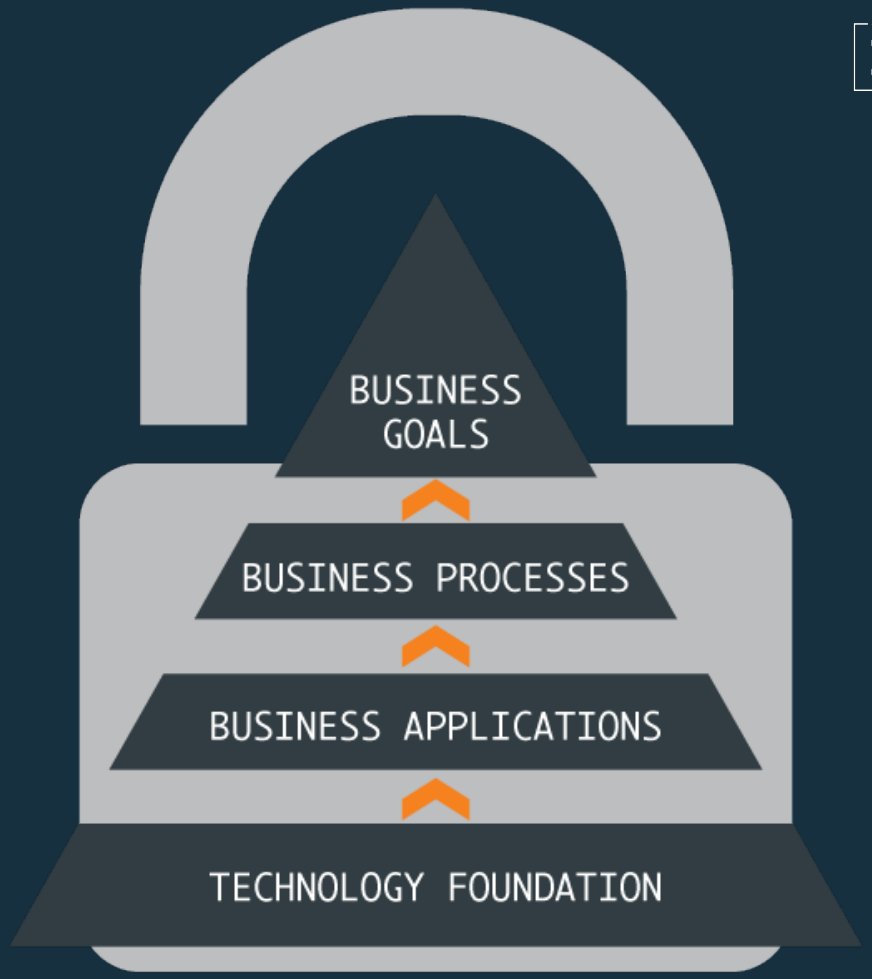
NINE THINGS YOU MUST DO TO PROTECT YOUR BUSINESS

JERRY HOOK, CTO

The ICG Approach

Technology plays a crucial role in the success and operations of businesses across all industries and sectors.

A solid **technology foundation** delivers your **business applications** when and where you need them. These two combined implements your unique **business processes** allowing you to reach your **goals**.



O U R M I S S I O N :

Deliver innovative and reliable business and technology solutions that exceed our client's expectations, resulting in reduced cost, improved efficiency, and a guaranteed ROI.

O U R V I S I O N :

Enable enterprises of all sizes to leverage technology for business growth and success.

HIGH LEVEL

Nine things you must do to protect your business.

1. **Stakeholder Support**
2. **Plan Your Goals**
3. **Design Organizational Conventions**
4. **Safeguards**
5. **Identify Security Event Criteria**
6. **Plan Security Event Activities**
7. **Restoration Post-Security Event**
8. **Know Your Enemy**
9. **Zero Trust Initiative**

STAKEHOLDER SUPPORT

PART ONE OF NINE

IDENTIFY AND GAIN SUPPORT

TOP EXECUTIVES

BOARD MEMBERS

Identify your stakeholders in this initiative to protect your business and then gain buy-in.

PLAN YOUR GOALS

PART TWO OF NINE

SECURITY BUSINESS GOALS

ESTABLISH BUSINESS SECURITY GOALS.

Plan short term goals.

Plan long term goals.

DESIGN ORGANIZATIONAL CONVENTIONS

PART THREE OF NINE

DESIGN SECURITY CONCEPTS INTO ORGANIZATIONAL CONVENTIONS TO HELP MANAGE RISK TO SYSTEMS, ASSETS AND DATA

Identify critical business processes and assets.

Confirm the most important items to Risk that must continue for the business to stay viable.

Document data flow, include type and location (fileserver, cloud, apps).

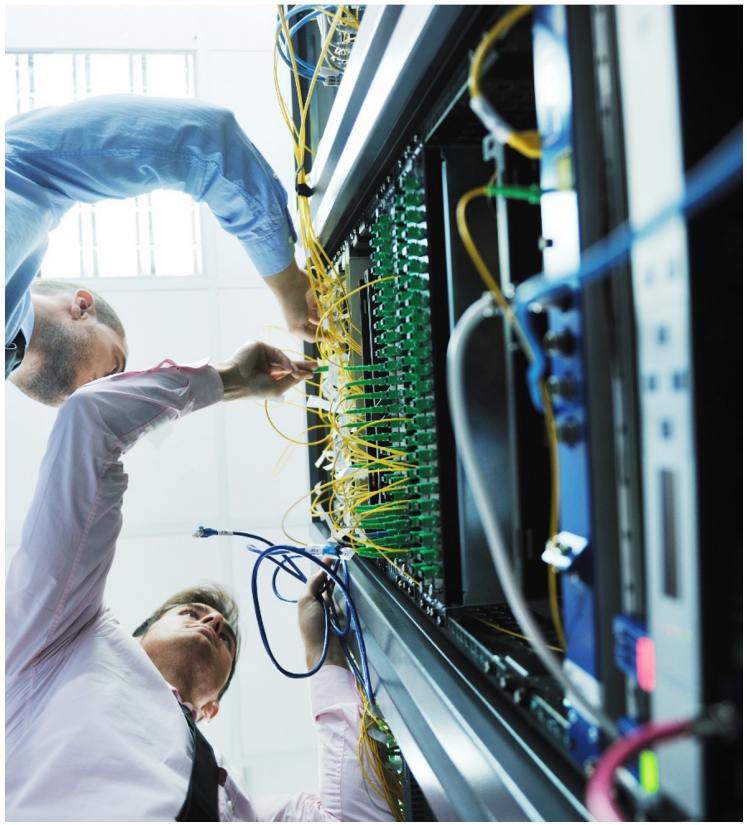
Develop policies and procedures on how to protect corporate data.

Maintain current hardware and software inventory, especially user workstations (these are frequently entry points for malicious actors).

Locations of assets accessing company systems.

SAFEGUARDS

PART FOUR OF NINE



DEVELOP AND IMPLEMENT THE PROPER SAFEGUARDS TO ENSURE DELIVERY OF SERVICES

Limit user access to only the systems and data required to perform their tasks. (Need to Know, Least privilege access)

Tightly manage access; require complex passwords and use MFA.

Protect sensitive data by encrypting data in flight and at rest; destroy data when no longer needed.

Design backups on-site, off-site with a complete set air-gapped or offline to protect from ransomware.

Install host-based firewall, endpoint security products.

Apply standardized configurations to devices.

Patch systems and manage vulnerabilities.

Train the user base often on user security protocols.

IDENTIFY SECURITY EVENT CRITERIA

PART FIVE OF NINE

DEVELOP CRITERIA AND IMPLEMENT ACTIVITIES USED TO IDENTIFY A SECURITY EVENT

Run penetration tests to test your system for vulnerabilities.

Monitor logs and look for anomalies using tools such as log servers or Siem tools.

Learn, map and document how your data is expected to be used in the enterprise.

Design policies and tools to quickly understand the breadth and depth of the impact to a security event.

Communicate criteria and activity information to stakeholders.

Develop security event response plans.

PLAN SECURITY EVENT ACTIVITIES

PART SIX OF NINE

DEVELOP CRITERIA AND IMPLEMENT ACTIVITIES USED TO TAKE ACTION DURING A DETECTED SECURITY EVENT

Test response plans.

Ensure each responsibility in a response plan is assigned and practiced to have a maximum effective response.

Include stakeholders to assist response plan evolution and improve execution.

RESTORATION POST-SECURITY EVENT

PART SEVEN OF NINE

RESTORE CAPABILITIES AND SERVICES IMPAIRED BY THE SECURITY EVENT

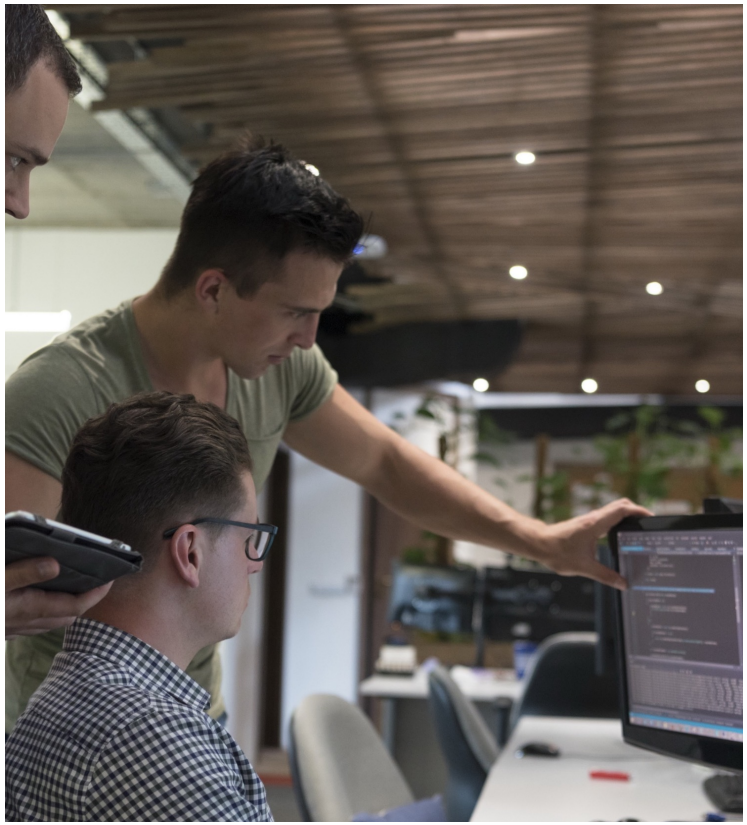
Communicate with stakeholders to co-develop a plan to mitigate future attacks and establish how business practices can help with the post-security event processes.

Identify refresh schedules to ensure all plans are updated to include system and plan evolution.

Manage public relations as required to secure company reputation.

Know Your Enemy

PART EIGHT OF NINE



KNOW THE TRENDS IN CYBERSECURITY AND HOW THEY AFFECT YOU AND YOUR COMPANY

91% of all security events start with Email.

Social Engineering is top vector

Ransomware continues to lead as highest cyberattack type, Reason :Money motivated!

Manufacturing: 1814 Reported Incidents 259 Breaches

Data Breach Incident Report: Talks about current Cyber Security trends.

ZERO TRUST INITIATIVE

PART NINE OF NINE

CONSIDER ZERO TRUST – A NEW SECURITY INITIATIVE

Zero Trust is the concept that nothing is trusted in or on the network, no matter where the requester is located.

Legacy approach to security design against security events is to harden the outside but leave the inside fully trusted inside.

Today, the new approach to security design against security events is to trust nothing unless you prove it.


TENNE