The Business of Cybersecurity

Date: September 2025

Presented by:

SIMPLI GRC

Agenda

1. Introduction
2. What is the Business of Cybersecurity?
3. What is the Challenge?
4. Symptoms of the Challenge
5. Root Cause(s)
6. Recommendations
7. Why Address the Challenges?
8. Conclusion

Introduction

1. Started 1999 in networking and troubleshooting
2. Project manager for +30 projects over +17 years
3. GRC and critical Infrastructure for +12 years
4. Certifications:
   - ISO/IEC 27001 Lead Auditor
   - ISO/IEC 27001 Lead Implementer
   - PMP
   - Security+
5. Partner and Co-Founder for SimpliGRC Inc.

Presentation Format

1. Intended for the technical audience
2. Open forum, encourage Q&A any time
3. Slide deck will be published on our website
4. Information presented may or may not apply to your org
5. Be cautious of sharing proprietary or confidential information, this is a public forum
6. No intent to diminish cybersecurity's role, only repositioning it
7. Information may be new to some, old to others

What is the Business of Cybersecurity?

NIST Definition for Cybersecurity:

- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

The Business of Cybersecurity

- Supports the organization's strategy, goals, and objectives as a cybersecurity function
- Protects the prioritized assets of an organization through cyber techniques, controls, and solutions
- Reduces cyber risk for the organization's prioritized assets and processes

What is the Challenge?

Scenario

- A large corporation owns and operates ~20k endpoints.
- A large percentage of the endpoints are MS Windows-based platforms
- Information Security policy require all critical and high security patches to be implemented within 2 days
- Patch Tuesday activities required a high degree of coordination every month
- Success metrics were based upon implementing the patches to all endpoints

What is the Challenge?

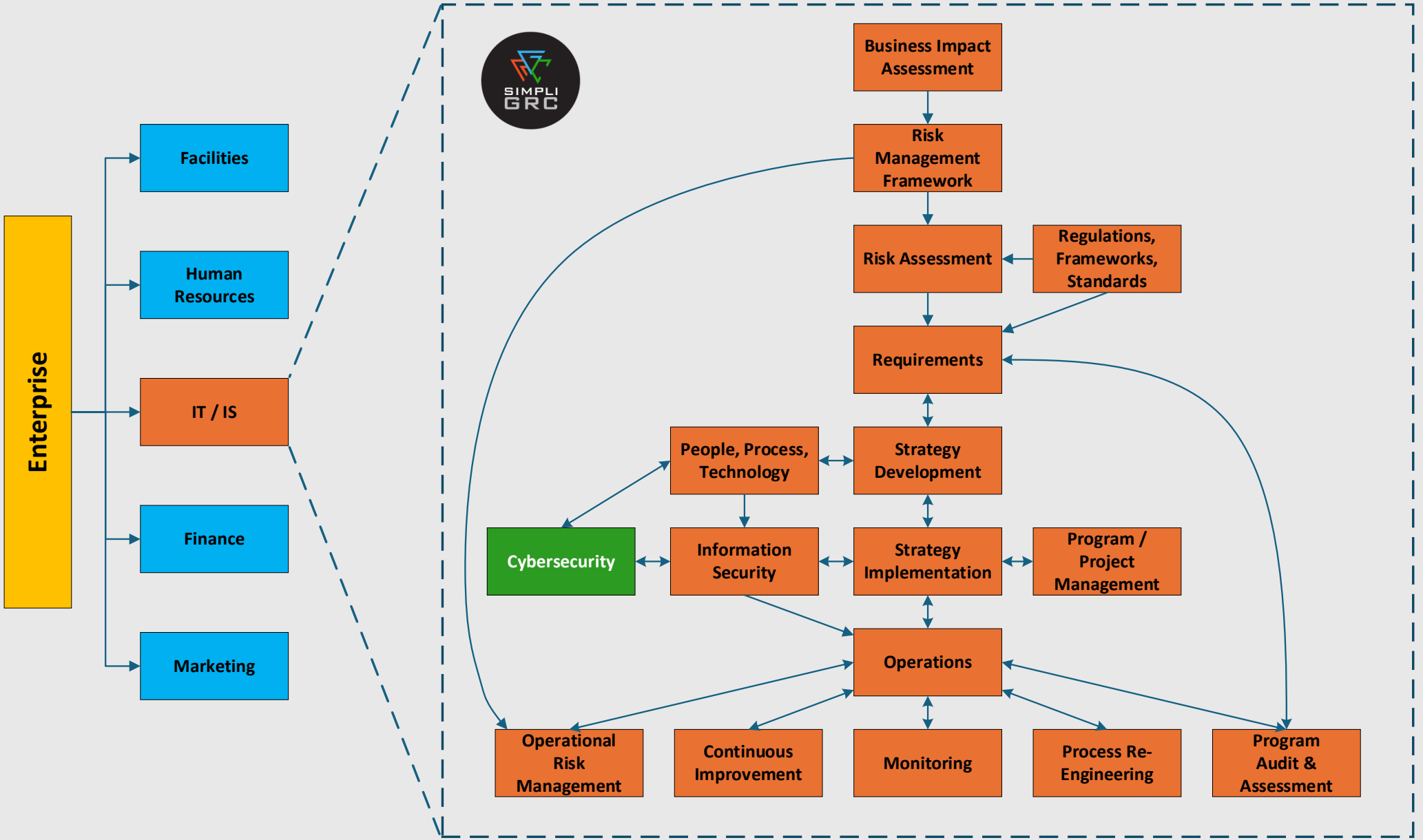
Scenario

- A large corporation owns and operates ~20k endpoints.
- A large percentage of the endpoints are MS Windows-based platforms
- Information Security policy require all critical and high security patches to be implemented within 2 days
- Patch Tuesday activities required a high degree of coordination every month
- Success metrics were based upon implementing the patches to all endpoints

Cybersecurity still operates in a silo in many organizations

- Cybersecurity is an enabler service to the business and its strategy
- Integration with the business is often overlooked
- Cybersecurity has formed its own culture without consideration to other cultures

A Sample GRC Program



Symptoms of the Challenge

Cybersecurity still operates in a silo in many organizations

1. Business processes are often restricted with cybersecurity requirements
   - Cybersecurity requirements may be prioritized over business requirements
   - Technical risks may be prioritized over business risks
2. Integration with the business is often overlooked
   - Many standards, frameworks, regulations require cybersecurity to support the business
   - “Checking the box” focus versus business value
3. People and process controls are often separated which can create an isolated or point-in-time cybersecurity solution
4. Business units may circumvent cybersecurity departments
   - Why does “shadow IT” exist?
5. A technical solution was implemented but business requirements still exist
   - Technical solutions are used to define your business or operations
6. Culture clashes between departments
7. Continuous exposure to increasing cyber threats and risks

Root Cause(s)

Cybersecurity still operates in a silo in many organizations

1. Leadership may:
    - not understand the value cybersecurity brings to the business
    - attend to competing priorities
    - have miscommunication
    - trust the cybersecurity function
2. The cybersecurity function is not integrated with the business
    - Mandate of the cybersecurity function is unclear
    - Focus are cybersecurity industry targets, not business targets
3. Trust can be confused with autonomy
4. Cyber tools are seen as solutions to problems – Remember people and process
5. Cybersecurity function acts as a business rather than a business enabler / service

Recommendations (1 of 4)

Create value through cybersecurity services

1. Use the risk management processes to communicate with the impacted stakeholders
   - Stats on security patches for critical systems where compensating controls are insufficient to reduce risk
   - Translate from a technical risk for a man-in-the-middle attack to what information can be exfiltrated and impact to strategy
2. Support the automation of people and process controls, not only technology
3. Contribute to the assessment of positive risks and reducing opportunity costs

Recommendations (2 of 4)

Derive cybersecurity targets from the enterprise goals

1. Evolve cybersecurity requirements from the business requirements.
2. Integrate cybersecurity into new business initiatives / functions like third party assurances, cyber maturity to increase client trust, and alignment with enterprise risks.
3. Prioritize cyber resources to the high-risk areas for the business.
    - Technical priorities are important but determine how they impact the business first.
    - Technical risks are important but should not be independent of the business.

Recommendations (3 of 4)

Shift reporting focus from cybersecurity to business

1. Learn the business language and environment and how cyber threats and vulnerabilities impact the critical assets.
   - Shift reporting from cybersecurity metrics to business applicable KPIs.
     - Phishing metrics are essential but translate the data to meaningful business information.
     - Report how business risks are reduced through platform standards or security patch levels.
2. Impacts to strategy, policies, operations, and compliance programs.
3. Incorporate the enterprise risk metrics, if they exist.

Recommendations (4 of 4)

Integrate into the business culture, not the reverse

1. Cyber typically is not a revenue source
2. Funding for cybersecurity comes from the departments that generate revenue
3. Become a trusted service to the business.
   - Implying the operations to prioritize cyber over operational priorities will reduce trust.

Why Address this Challenge?

Cybersecurity still operates in a silo in many organizations

1. Business goals and strategies change
    - Other departments adjust, cyber is no different
    - Organizations must do more with less
    - Acquisitions and mergers
    - Outsourcing services
    - Increased competition and innovation
    - Political and regulatory environments change
    - Economic (Boom & Bust) cycles

2. The external environment is ever-changing
    - Artificial Intelligence are replacing workforce tasks
    - Quantum Computing will disrupt the cybersecurity industry
    - State-actors and other organized threats are evolving
    - The digital world continues to grow bigger and stronger

3. Relations with leaders improve
    - Contribute cybersecurity outcomes that positively impact the business goals
    - Work with the culture, not the reverse. Avoid unnecessary bureaucracy and office politics

Conclusion

1. Understand that cybersecurity is part of the larger system.
2. Cybersecurity must support the business as all the other departments support.
    - Imagine if marketing and finance departments did not support the business.
3. The cybersecurity function is responsible to understand the business and provide value-added service.
    - Discuss with leadership in business terms, not technical or cyber.
    - Contribute to keeping the lights on.
    - Reduce cyber risk to the business objectives.
    - Develop cybersecurity metrics that align / support the business KPIs.
4. If cybersecurity is everyone's job, why do silos still exist?
5. Continue the cybersecurity work, extend further to integrate with the business.

CONTACT US

info@simpligrc.com

https://simpligrc.com