CyberTrends: Protect Your Business With Cost-Effective 360° Security Testing

Achieving comprehensive risk management through 7 distinct measurement actions

August 26, 2021

Presenter

Doug Davidson, CISA

Director of Information Technology Services

(614) 947-5340

ddavidson@gbq.com

Objectives

- The importance of ongoing security testing
- Selecting the right test
- Implementing an effective scheduling cadence
- Discuss testing cost containment
- Discuss testing relationship to regulatory requirements

GBQ Information Technology Services

Digital Strategy

Risk

- Governance, Risk, Compliance & Privacy
- Cybersecurity
- Digital Forensic & Incident Response

Productivity

- Data Analytics
- Process Automation
- ERP

IT Audit & Assurance

The Current Landscape

Why Have This Conversation?

- Security industry jargon is confusing
- No universal testing standards
- Firms often shop and / or buy the wrong things
- Firms do not conduct enough testing or the right testing because of the confusion

Cyber Top Causes of Loss

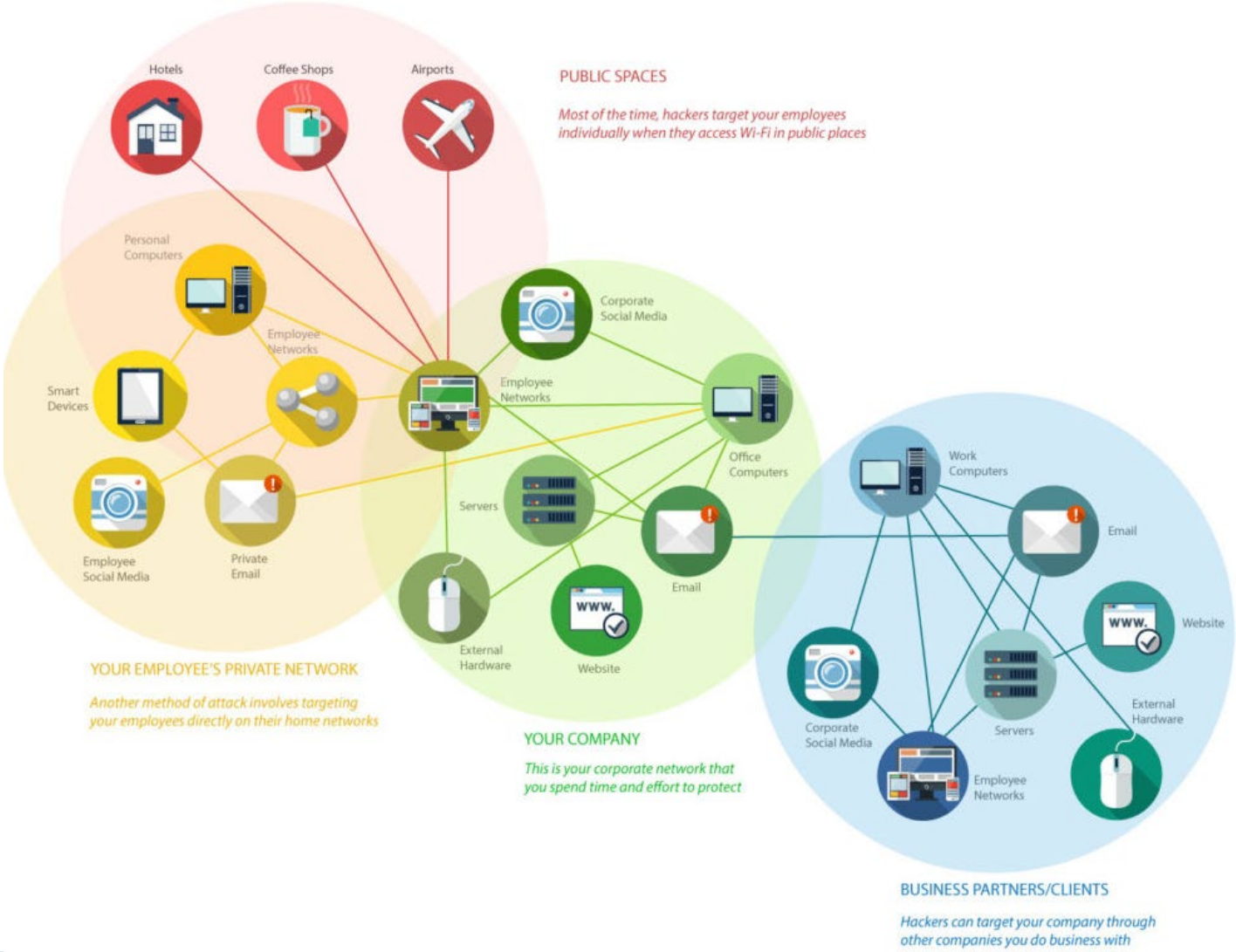
RANSOMWARE
When your information is held hostage, can you recover?

SOCIAL ENGINEERING
Being tricked into paying money to a fraudster

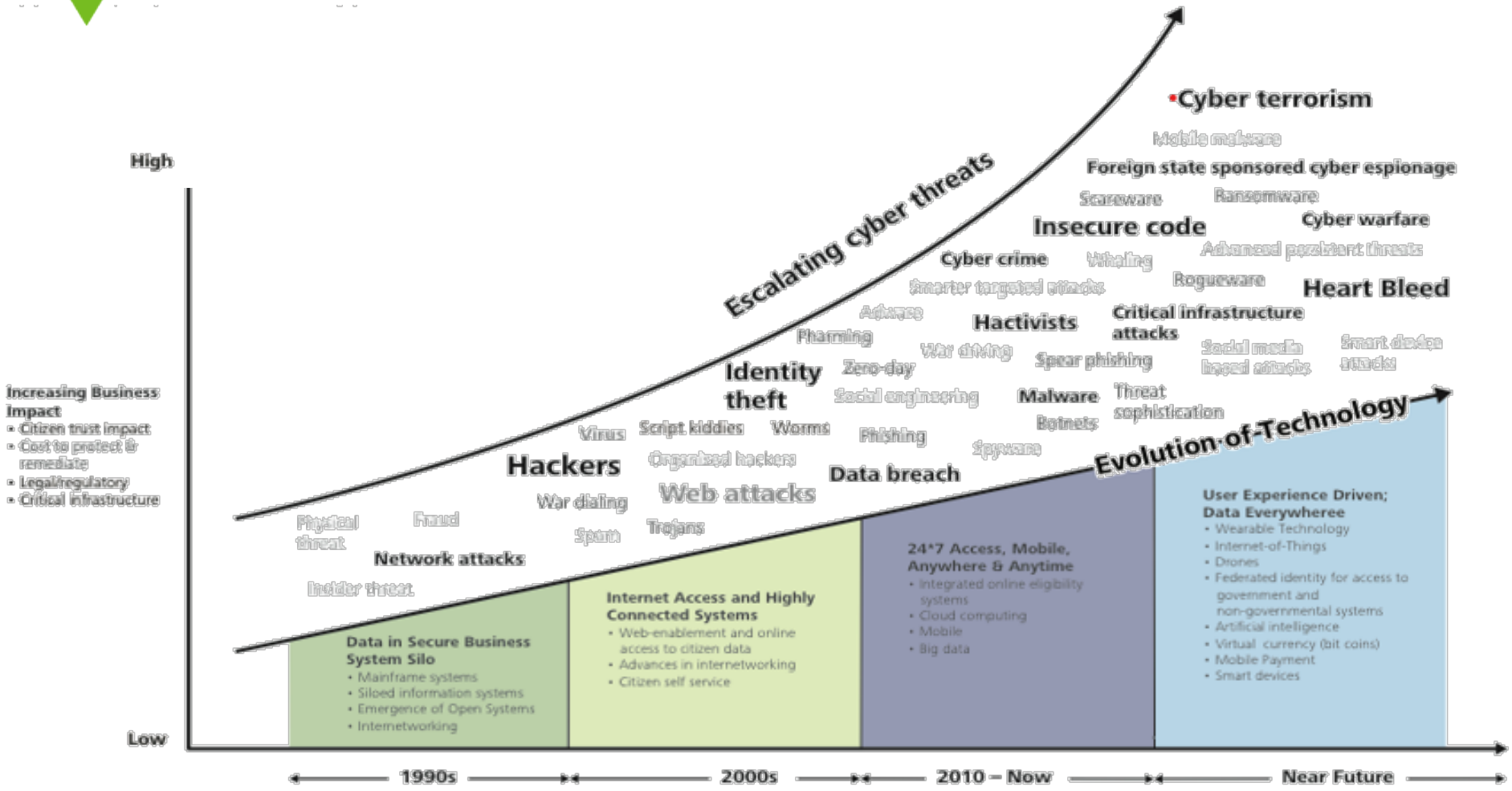
THIRD PARTY VENDORS
Cyber attacks on Cloud/IT Provider/Credit Card Processors impacting our insured

EMPLOYEES
Click on phishing emails

Attack Surfaces Are Expanding



Threats Evolve as Technology Evolves



Assess Everything!

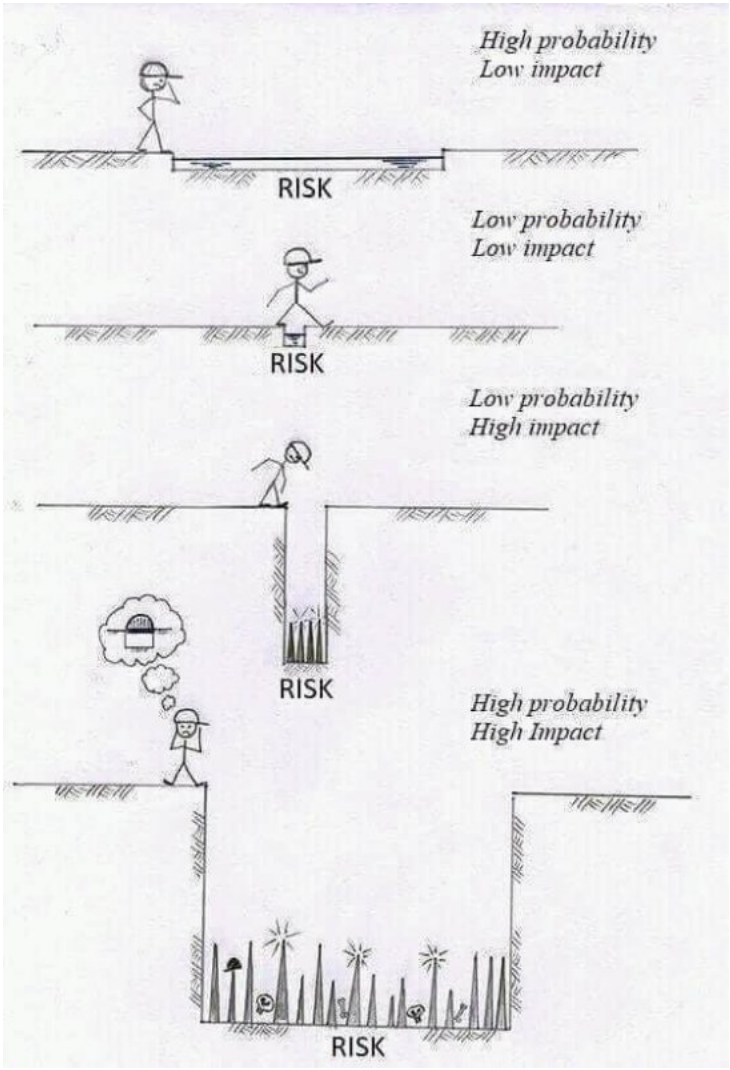
Assess → Improve → Manage

1. Assess
   - Risk
   - Program
   - Compliance
   - Controls
   - Vulnerability

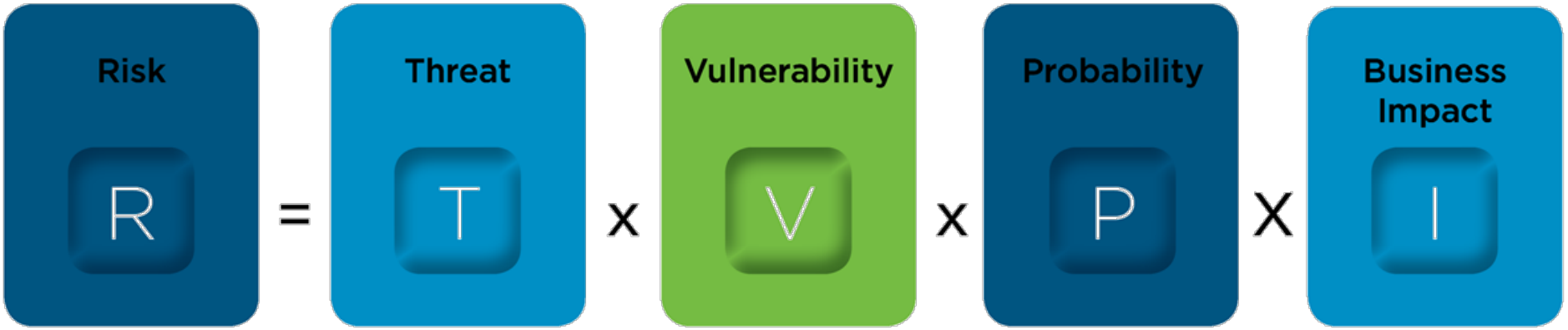
2. Improve (Remediation)
   - Safeguards
   - Program Performance

3. Test, Manage, Assure
   - Program Management
   - Penetration Testing
   - SOC Examinations

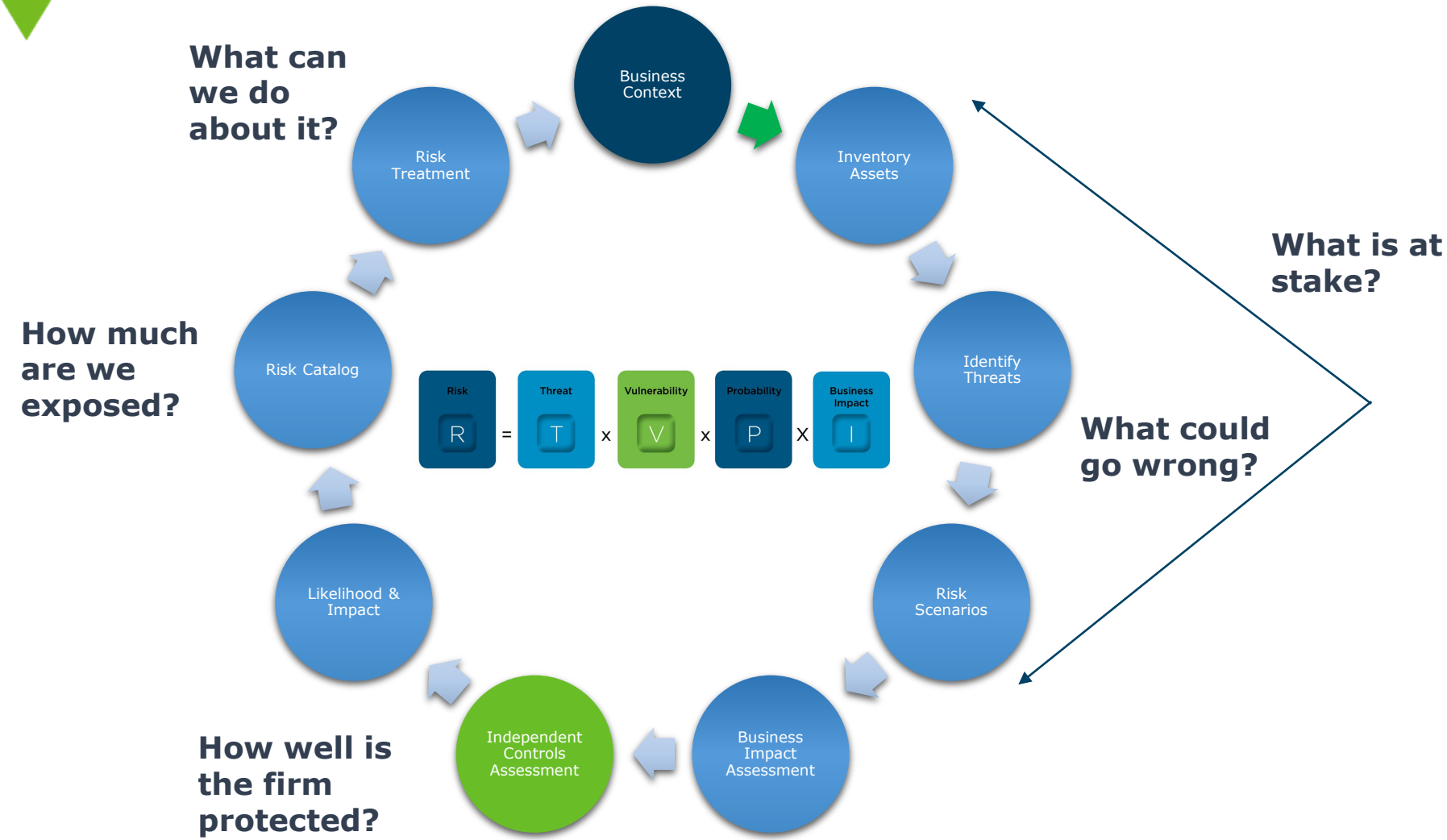
It’s All About Risk



It’s All About Managing Risk



Risk Assessment

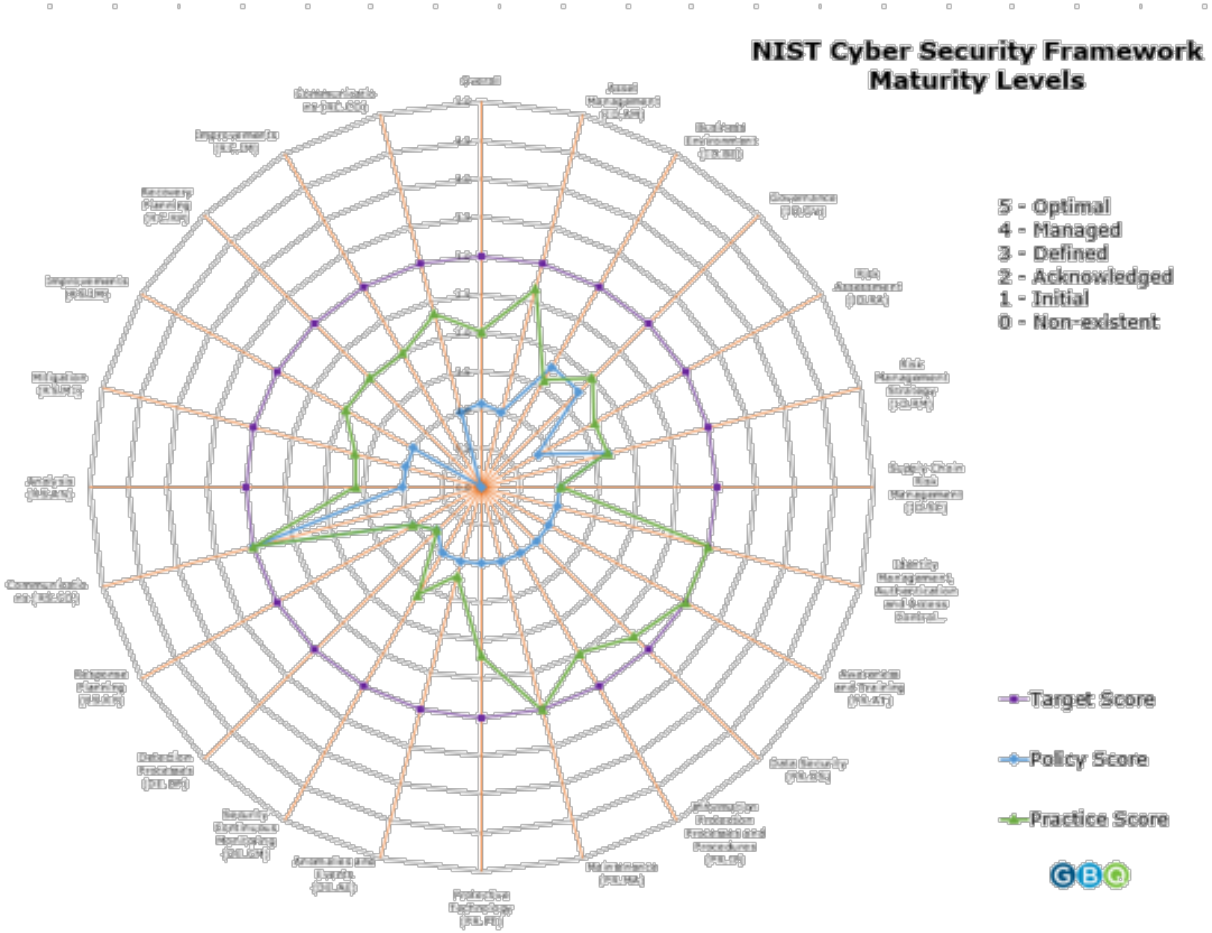


Program Assessment

Measure People, Process, Technology Inputs not just controls, risks or vulnerabilities

Measured in terms of maturity:

- Practices – things we do
- Policy – statements of value that document practices we say we should follow



GBQ

Control & Compliance Assessments

Control Assessment	Compliance Assessment
Identify the security controls in place against a identified control framework We recommend firms select a control framework to organize their security program around	Measures alignment with external requirements by regulatory body or contract obligation
Examples: • NIST Cybersecurity Framework • CIS Controls • NIST 800-53 • ISO 27001	Regulatory Examples: • HIPAA • CMMC • FFIEC Contractual Examples: • PCI • Customer Contract
Some frameworks include other tests as controls (e.g. vulnerability scanning / assessment, penetration testing)	Some authorities include other tests as controls (e.g. HIPAA – Security Risk Assessment; CMMC – Risk Assessment; PCI – Penetration Testing)

Vulnerability Assessment / Scans / Scanning

Why do we do it?

- Identify vulnerabilities (weaknesses) and configuration issues that may put the organization at risk of being compromised or exploited
- Identify attack vectors most likely to be successfully compromised
- Meet compliance requirements

How do we do it?

- Automated vulnerability scans (host, application, etc.) with expert analysis
- Manual analysis (phishing simulations)

What's the end result?

- Documented list of weaknesses ranked by severity

Practice:

- Vulnerability Assessments should be a frequent and ongoing process to continuously monitor and identify weaknesses in an organization and reduce the attack surface
- Consider self managed vulnerability management systems or a 3rd party scanning bureau rather than infrequent Vulnerability Assessments

Assess All the Things

Type	Purpose	Deliverable	Audience
Assess			
Risk Assessment	Identify what is at stake, what could go wrong, how well is the firm protected, how much is the exposure, what to do about it	Risk Assessment Control Assessment Vulnerability Assessment	Board, Executives, Technology Leadership
Program Assessment	Demonstrate how security is refined in an organization. Shows that security maturity takes time to be part of an established organization and how an organization can transform from viewing security as a cost to an investment. Measure People, Process, Technology Inputs not just controls, risks or vulnerabilities	Maturity Assessment	Board, Executives, Technology Leadership
Compliance Assessment	Measure external requirements by standard/regulatory bodies Cost of doing business	Compliance Gap or Readiness Assessment	Board, Executives, Technology Leadership Regulatory Authority
Control Assessment	Identify the security controls we already have in place against an identified control framework Understand where we might have gaps and what must be done to close them	Control Framework Assessment	Board, Executives, Technology Leadership
Vulnerability Assessment	Emulate attack scenarios identified during the risk assessment Validate the effectiveness of implemented controls	Vulnerability Analysis or Scan	Technology Leadership, Technology Doers

Improve your Posture

Assess → Improve → Manage

1. Assess
   - Risk
   - Program
   - Compliance
   - Controls
   - Vulnerability
2. Improve (Remediation)
   - Safeguards
   - Program Performance
3. Test, Manage, Assure
   - Program Management
   - Penetration Testing
   - SOC Examinations

Improve (Remediation)

- Invest to reduce risk
- Work from a risk catalog (risk register) that prioritizes (impact x likelihood) remediation actions to take
- Focus on Critical and High Risks First
- Work to remove the root cause NOT just the finding
- Allow enough time to remediate before the next test
    - If a test produces more findings than you can cure in 90 - 180 days adjust to conduct smaller, more frequent tests
- Test or audit to validate the remediation effort

Test Your Posture

Assess → Improve → Manage

1. Assess
   - Risk
   - Program
   - Compliance
   - Controls
   - Vulnerability

2. Improve (Remediation)
   - Safeguards
   - Program Performance

3. Test, Manage, Assure
   - Program Management
   - Penetration Testing
   - SOC Examinations

Penetration Test

What is it?

- Using attack (hacking) techniques to test an environment
- Breaking in for good to identify where someone may break in for bad

Why do we do it?

- Emulate attack scenarios a firm is concerned about
  - ✓ From risk assessment findings
  - ✓ From attack patterns "in the wild" – the news
- Validate the effectiveness of implemented controls

How do we do it?

- Manual or automated exploit attempts (manual control of a pentesting platform)

What's the end result?

- Confirmation of vulnerabilities
- Refined list of exposures most likely to result in a compromise

Selecting the Right Penetration Test

- What is the pen test strategy?
- What is the involvement of internal resources?
- What type of test?
- What are the reporting requirements?

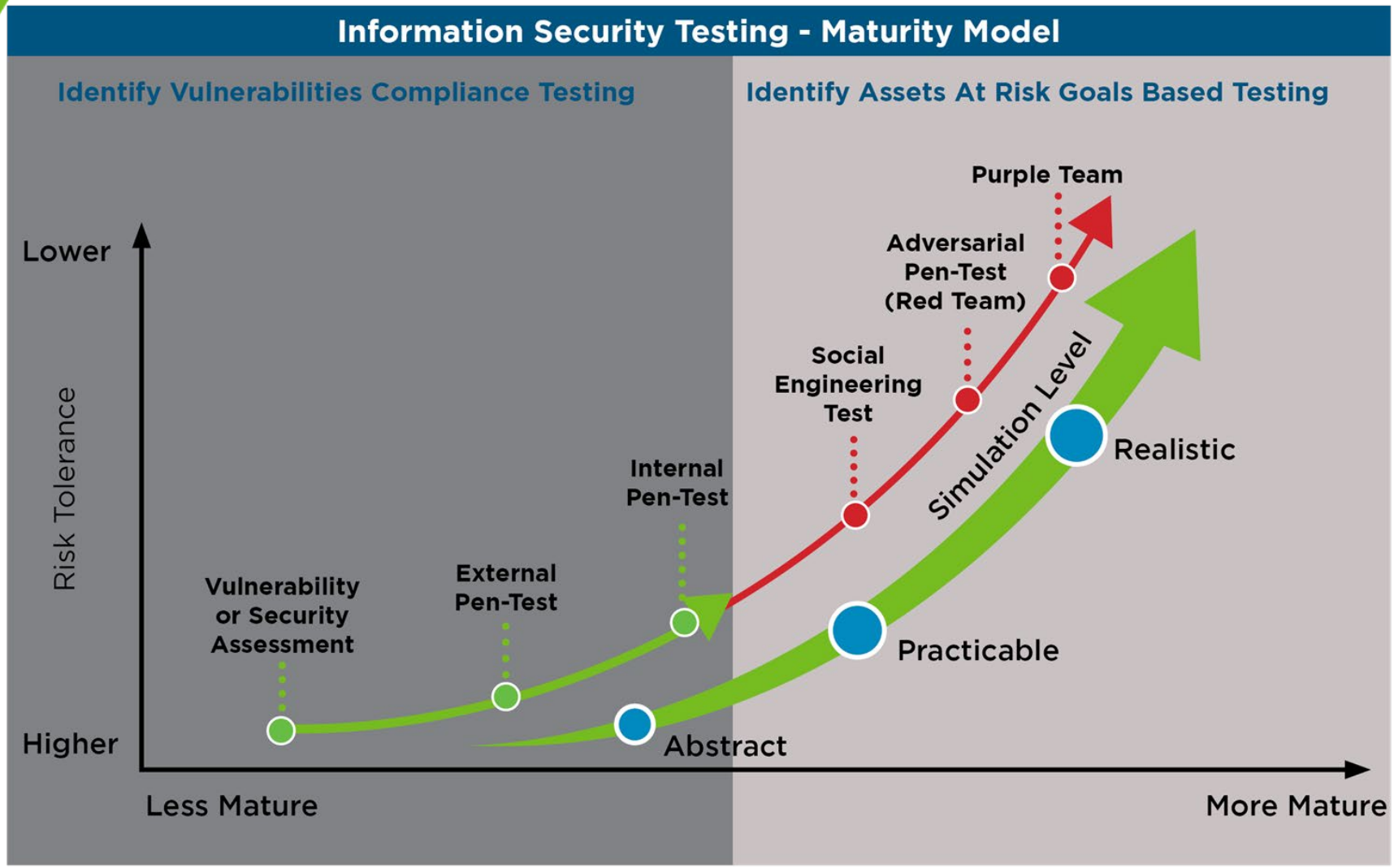
What is the Penetration Testing Strategy?

- **Compliance focused** – minimal testing focused on meeting specific requirements for compliance – PCI, SOC controls, customer requirements
- **Asset focused** – classic Vulnerability Assessment / Penetration Test focused on vulnerability identification & verification
- **Goal oriented** – purposeful testing; generally aggressive, adversarial styled testing measuring the organization's ability to prevent, detect, and respond to a real-life cyber-attack.
    - Assumed breach – Can the organization detect and remove a command & control (C2) infection?
    - Detection & Response capabilities – Can the organization detect and respond attacks? Are 3rd party security providers meeting contract service agreements? Are detective controls working?
    - Insider-Threats - what risks to insider threats pose to the organization?
    - Network Isolation – are key segments of the corporate network properly isolated from other segments?
    - Is the organization vulnerable to a ransomware attack?
    - Can a physical breach of the company lead to a cyber-attack?

Deep and Broad Testing Choices

Type of Test	Cost Variables
Compliance Network Penetration Test (Vulnerability Assessment Penetration Test) PCI Penetration Testing FI Penetration Testing	# of targets / locations Reporting
Device or Form Factor Specific Test	Form Factor Estimated testing time Reporting
Application Penetration Test	Application size # of roles to test from Reporting
Social Engineering Test	# of employees to test Address book test v. targeted test
Adversarial Penetration Test	# of identified goals to best Estimated testing time Reporting
Assumed Breach Pen Test	# of assumed scenarios Estimated testing time Reporting
Purple Team Test	Rigor of test Estimated testing time Reporting
Red Team Test	# of systems Frequency of testing

Spectrum of Penetration Testing Choices



What is the Company Staff Involvement?

- **Overt**- These pen-tests are those performed with the knowledge and consent of IT staff and, of course, upper management.

- **Covert** - involves performing a pen-test without the knowledge of IT staff, but with consent from upper management. Not announcing pen-testing helps the organization to check the security threats that arise due to human errors and ignorance. It also examines the agility of the security infrastructure and the responsiveness of the IT staff.

What are the Reporting Requirements?

- **Light documentation**
  - Executive Summary only
  - Risk Register (light documentation)
  - Evidence gathered including scan outputs (if scans)

- **Detailed Reporting**
  - Executive Summary, Technical Summary, Detailed Technical Analysis
  - Risk Register
  - Evidence gathered including scan outputs (if scans)

- **Key questions:**
  - What is the purpose of the documentation?
  - Who is the audience?
  - Will a customer-facing letter be required?

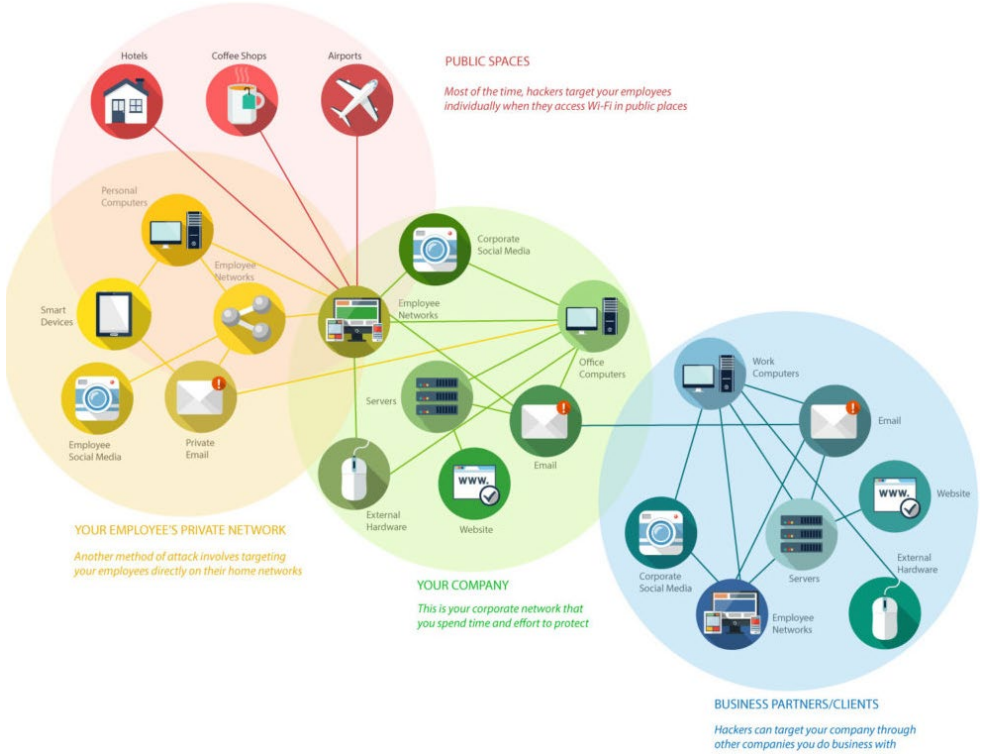
What type of Penetration Test?

- **White** box —All information that testers need to exploit vulnerabilities is provided. This option is preferable when:
  - The scoping task is left to the testers to determine
  - Vulnerability focused testing covering the full breadth of systems.
  - Organizations want to simulate an attack from an inside threat, such as a disgruntled IT employee who would already have access to such information
- **Black box** —No information is shared with the testers. This simulates an external attack where testers will spend more time in the reconnaissance phase and, because of that, it tends to take more time and be more expensive.
- **Grey box** —Some information is provided to the testers—that which hackers would, perhaps, obtain when using reconnaissance tools or after obtaining access to local area networks (LANs). This decreases the time spent by the testers and, therefore, cost as well. Information given does not compromise the pen-test's validity. Examples of such information would be a list of out-of-scope hosts or a lighter version of network topology.

Identify the Attack Surface

What is the **attack surface** to be tested?

- Internal
- External
- Cloud
- Applications
- Mobile Devices
- Industrial Control Systems
- IoT devices
- Third Parties
- Physical
- Social (Individuals)



Audits

What is it?

- An examination of the management controls within an Information technology (IT) infrastructure and business applications.

Why do we do it?

- When we need an independent opinion on whether or not we are following our selected and defined controls

How do we do it?

- Evaluating controls by sampling control activity to assure controls are being followed

See GBQ CyberTrends: The Ins and Outs of a SOC Examination (https://gbq.com/wp-content/uploads/2021/03/3-18-21-The-Ins-and-Outs-of-a-SOC-Examination.pdf)

Assess All the Things

Type	Purpose	Deliverable	Audience
Test & Assure			
Penetration Test	Emulate attack scenarios identified during the risk assessment Validate the effectiveness of implemented controls	Penetration Test Report	Board, Executives, Technology Leadership / Doers
Audit	When we need an independent opinion on whether or not we are following our selected and defined controls	Audit Examination Report	Board, Stakeholders such as customers, prospects

Considerations Before Assessing

Cost Containment

- Don’t over assess, under remediate
  - ✓ If you can’t keep up with remediation, choose smaller more frequent tests
- Documentation costs are a heavy part of delivery process
  - ✓ Lighter, actionable reporting such as risk register only if improvement is main purpose
  - ✓ Heavy analytical report if project is for regulatory or internal control purposes
- Consider Self Assessment v. Third Party Assessment
  - ✓ Vulnerability Management v. Vulnerability Assessment
  - ✓ Self Phishing (KnowBe4) v. Social engineering penetration test
- Negotiate away from the audit until stakeholders give you no choice
- Be organized regardless of the assessment type
  - ✓ Security & compliance requires good organization
  - ✓ Spending staff time to document systems to be tested, find key policy & other documentation often adds to client costs

Testing Cadence – Leading Practice

- Annual Risk Assessment which should include:
  - Control framework assessment against your selected framework
  - Vulnerability Assessment of entire company attack surface
- Consider implementing vulnerability management as a company operated control
  - Implement the tools (i.e. Qualys, Tenable) to conduct your own routine vulnerability scans
  - Engaging a scanning bureau to run the scans for you
- Conduct compliance assessments as dictated by your regulatory obligations
- Conduct an annual penetration test (6 months after Risk Assessment)
- Conduct other tests as facilities, staffing, processes change (trigger events)
- Select audits are regulators, customers, prospects or other third-party stakeholders require them

Testing Triggers -- Timing

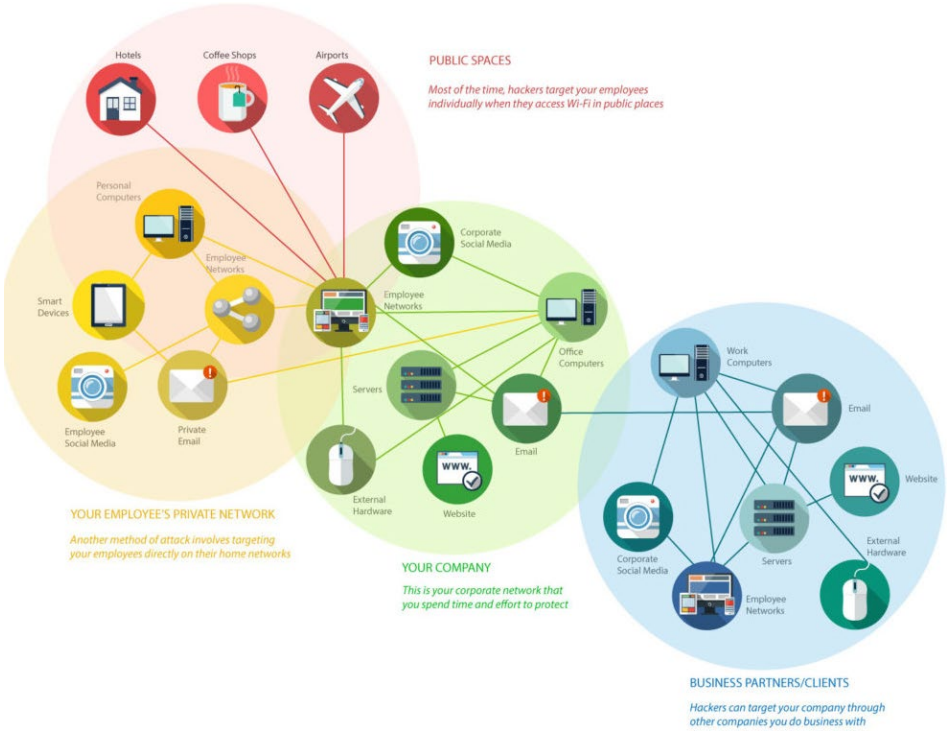
Some of the objectives and occasions for conducting a pentest are as follows:

- New vulnerability released
- Network/application / facility change
- Vulnerability management program:
  - Routinely based on firm policy
  - At least annually (penetration test) / at least quarterly vulnerability testing / at least annually vulnerability assessment
- Application launches
- Major network/application change or update
- Vulnerability management program
- Compliance regulations / requirements
- After a breach or leak

Identify the Attack Surface

What is the **attack surface** to be assessed, audited, or tested?

- Internal
- External
- Cloud
- Applications
- Mobile Devices
- Industrial Control Systems
- IoT devices
- Third Parties
- Physical
- Social (Individuals)



Assess All the Things

Type	Purpose	Deliverable	Audience
Assess			
Risk Assessment	Identify what is at stake, what could go wrong, how well is the firm protected, how much is the exposure, what to do about it	Risk Assessment Control Assessment Vulnerability Assessment	Board, Executives, Technology Leadership
Program Assessment	Measure People, Process, Technology Inputs against not just controls, risks or vulnerabilities	Maturity Assessment	Board, Executives, Technology Leadership
Compliance Assessment	Measure external requirements by standard/regulatory bodies Cost of doing business	Compliance Gap or Readiness Assessment	Board, Executives, Technology Leadership
Control Assessment	Identify the security controls we already have in place against an identified control framework Understand where we might have gaps and what must be done to close them	Control Framework Assessment	Board, Executives, Technology Leadership
Vulnerability Assessment	Emulate attack scenarios identified during the risk assessment Validate the effectiveness of implemented controls	Vulnerability Analysis or Scan	Technology Leadership, Technology Doers
Test & Assure			
Penetration Test	Emulate attack scenarios identified during the risk assessment Validate the effectiveness of implemented controls	Penetration Test Report	Board, Executives, Technology Leadership
Audit	When we need an independent opinion on whether or not we are following our selected and defined controls	Audit Examination Report	Board, Stakeholders such as customers, prospects, regulators

Questions?

Contact Information

Doug Davidson, CISA

Director of Information Technology Services

(614) 947-5340

ddavidson@gbq.com