BUILDING AND SELLING YOUR SECURITY STRATEGY: A CASE STUDY

Rick Patterson
Head of Security Operations
Financial Services
@rpatterson123
Overview

- Why is this important
- How (Case Study-ish)
  - Build a risk Framework
  - Get Business buy-in
  - Customize a Control Framework
  - Develop Tooling
- Benefits to your Organization
- Key takeaways
- Application
Why is this important

- It is the building block for a risk based security strategy
- Helps answers questions on why you need funding and for what
- Protects your budget
- Source of additional funding for critical risk remediation
- Helps answers threat questions within a framework
- Protects you and your team from being the fall guy (unless you deserve it)
How to sell our security strategy

- Four critical components
  - Risk Framework
  - Business buy-in/support
  - Customized control framework
  - Tooling
Risk Framework

Current Goal

- Develop an enterprise risk picture that will help identify and prioritize initiatives to drive down risk across Bridgewater (i.e. what controls do we invest in)

Current Scope

<table>
<thead>
<tr>
<th>Enterprise Risk Domains¹</th>
<th>Operational Risk Domains²</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Risk</td>
<td>Technology Risk</td>
</tr>
<tr>
<td>Reputational Risk</td>
<td>Security</td>
</tr>
<tr>
<td>Financial Risk</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Third Party Risk</td>
</tr>
<tr>
<td>Liquidity Risk</td>
<td>Internal/External Fraud</td>
</tr>
<tr>
<td>Market Risk</td>
<td>Data Privacy Risk</td>
</tr>
<tr>
<td>Capital Risk</td>
<td>Processing Risk</td>
</tr>
<tr>
<td>Credit Risk</td>
<td>Human Capital Risk</td>
</tr>
<tr>
<td>Legal / Comp. Risk</td>
<td>Project Risk</td>
</tr>
</tbody>
</table>
Risk Framework

Risk Identification
1 External party takes down systems / causes denial of service
2 External party steals / exfiltrates pending trades
3 Authorized Employee misuses knowledge of Top Secret data
4 Employee leaks client information

Risk Assessment
Analyze + classify those risk scenarios ...

Control Mapping
Understand controls needed to address risk

Prioritize and Define Initiatives
Build/improve controls that drive down risk

Prioritize Perceived Risks and Control Gaps
2 External party hacks BW and steals / exfiltrates TS data
3 Authorized Employee steals / misuses their knowledge ...
4 Employee physically steals TS data

Initiatives that Address Risks
Project A and B
These projects are designed to reduce risk 2 and 3 respectively

Initiatives that Increase Confidence
Project C
This project is designed to increase the confidence for a potentially high impact risk
Business buy-in/Support

Enterprise Risk Assessments

1. Captured department risks with Security SME’s.
2. Conducted Risk Workshops with DH.

Key to Success

• Get buy-in from the business
• Keep it simple and interactive
• Establish clear rules of the road
• Cut off debate
Enterprise Risk Assessments

**IMPACT**

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
<th>Description</th>
<th>Reputational / Customer</th>
<th>Impact (1-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Very High</td>
<td>Potential existential impact to BW</td>
<td>• Extreme impact on client perception and experience</td>
<td>• Devastating financial loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Devastating loss of clients and market share</td>
<td>• Significant, permanent impact to revenue generation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• International long-term, negative media coverage</td>
<td>• Potentially existential</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>Serious, long-term impact to BW</td>
<td>• Major impact on client perception and experience</td>
<td>• Major financial loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Loss of clients and market share</td>
<td>• Reduced ability to generate revenue going forward</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• National long-term, negative media coverage</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Material but recoverable impact</td>
<td>• Significant impact on client perception and experience</td>
<td>• Moderate financial loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Some impact to attract and retain clients</td>
<td>• Near-term revenue loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• National short-term, negative media coverage</td>
<td></td>
</tr>
</tbody>
</table>
### Enterprise Risk Assessment

#### Likelihood (1-5)

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
<th>For Adversarial Risks (i.e. Security Attacks)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Very High</td>
<td>The risk is <em>almost certain</em> to occur. The event occurs regularly at BW or similar firms.</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>The risk is <em>highly likely</em> to occur. There is a strong possibility the event will occur as there is a history of occurrence at BW or similar firms.</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>The risk is <em>somewhat likely</em> to occur. The event may occur at some time and has happened at BW or similar firms.</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>The risk is <em>unlikely</em> to occur. Not expected, but there's a slight possibility it may occur at some time.</td>
</tr>
<tr>
<td>1</td>
<td>Very Low</td>
<td>The risk is <em>highly unlikely</em> to occur. It may occur in rare, exceptional circumstances. It could happen, but probably never will.</td>
</tr>
</tbody>
</table>
## Risk Framework – Confidence

### Table

<table>
<thead>
<tr>
<th>CONFIDENCE - IMPACT</th>
<th>CONFIDENCE - PROBABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

### Legend
- **IMPACT**
  - Medical emergency
  - Security breach
  - Financial loss
  - Legal consequences
- **CONFIDENCE - IMPACT**
  - High
  - Medium
  - Low
- **CONFIDENCE - PROBABILITY**
  - High
  - Medium
  - Low

---

RSA Conference 2018
Security Control Framework

Customized taxonomy used to categorize our controls

Control Family
High level grouping/program of security controls

Control Objectives
Purpose/aim of controls being implemented across the organization

Control Requirements
Specific requirements that must be met in order to achieve higher level control objectives

Control Solutions
Specific technologies, processes, and tools that are implemented in order to support security objectives and requirements

ID | Control Family
---|------------------
1  | Security Strategy
2  | Risk Management
3  | Policy & Standards
4  | Audit
5  | Staff Security
6  | Physical Security
7  | Security Culture & Training
8  | Supply Chain
9  | Business Continuity Management
10 | Threat Intelligence
11 | Information Sharing and Communications
12 | Incident Response
13 | Monitoring
14 | Network Security
15 | Compute Security
16 | Vulnerability & Patch Management
17 | Asset and Configuration Management
18 | Identity and Access Management
19 | Data Protection
20 | Secure System Development

1. Security Control Framework has been developed using a number of industry standards and references for security controls, including: NIST, Cobit, ISO, and CIS/SANS.
Control Frameworks – SCF / DYNAMIC DOT

Security Control Framework

Control Families

1. Security Strategy
   Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for security activities in a manner that aligns security objectives with the organization’s strategic objectives and the risk to critical information assets.

2. Risk Management
   Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cyber threats to the organization, including its business assets, vulnerability, and exposure to external factors.

3. Policy & Standards
   Establish and maintain an enterprise policy and standards program that reflects applicable laws, regulations, and policies with security strategy.

4. Audit
   Establish, operate, and maintain an enterprise audit program that reviews and assesses critical effectiveness of existing business programs. The results, reports, and findings of audits are disseminated to the appropriate entities.

5. Staff Security
   Establish, operate, and maintain a program that establishes a risk-based posture of policy throughout the organization, governing a broad scope of individual behaviors and mitigating unacceptable risks through an effective governance process.

6. Physical Security
   Establish and maintain plans, procedures, technologies, and controls to protect personnel, hardware, programs, networks, and information assets and systems that could result from loss or damage to the organization.

7. Security Culture & Training
   Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity awareness and to ensure the ongoing comprehension of personnel, communication with the risk to critical infrastructure and organizational objectives.

8. Supply Chain
   Establish and maintain controls to manage the cybersecurity risks introduced by third-party providers and services of the organization.

   Establish, operate, and maintain plans for the continuity of essential staff, critical infrastructure, and business functions within the organization.

10. Threat Intelligence
    Establish, operate, and maintain an organization-wide threat management program to detect, analyze, and mitigate threats to the organization.

11. Information Sharing and Communication
    Establish, operate, and maintain relationships with internal and external entities to share and provide cybersecurity information, including vulnerabilities, to reduce risks and to increase operational effectiveness.

12. Incident Response
    Establish, operate, and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to test the effectiveness of cybersecurity policies and procedures.

13. Monitoring
    Establish and maintain activities and technologies to detect, analyze, and respond to cybersecurity events and to test the effectiveness of cybersecurity policies and procedures.

14. Network Security
    Establish and maintain plans, procedures, and technologies to identify, analyze, and respond to cybersecurity events and to protect the organization’s network infrastructure.

15. Computer Security
    Establish, operate, and maintain an enterprise computer security program that integrates security controls into the organization’s processes and procedures.

16. Vulnerability Management
    Establish and maintain plans, procedures, and technologies to identify, analyze, and respond to cybersecurity vulnerabilities and threats to the organization’s network infrastructure.

17. Asset and Configuration Management
    Manage the organization’s assets, both hardware and software, commensurate with the risk to the organization’s infrastructure.

18. Identity and Access Management
    Establish and maintain systems to control access to the organization’s assets and services.

19. Data Protection
    Establish, operate, and maintain a data protection program that protects the data itself and the technology infrastructure that supports access and use.

20. Secure System Development
    Establish, operate, and maintain a software development program that produces software that is secure and reliable.
Control Frameworks
Tooling
Control Mapping and Ratings
Control Mapping – Kill Chain analysis

Risk → Threat Vectors → Assets
Tool – Risk Library and Dashboard

Dynamic Control Prioritization
Bank of the Ozarks Risk Management Tooling

## Cybersecurity Risk and Control Maturity Assessment

### RISK SUMMARY

**February 21, 2018**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Inherent Risk</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Decreasing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Risk of unauthorized access to confidential information from unauthorized and unmanaged devices</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>17. Risk that employees are not aware of cyber security threats</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>19. Risk of data loss or corruption by undetected intruders</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>20. Risk of data loss due to an undetected security control gaps</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>4. Risk of unauthorized access to confidential information from unidentified threats and vulnerabilities</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>5. Risk of unauthorized access to confidential information from unauthorized and unmanaged administrative privileges</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>6. Risk that security audit logs are not used in cybersecurity management</td>
<td>Elevated</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Increasing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Risk of unavailable information due to Ransomware (or other malware) and inadequate recovery mechanisms.</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>13. Risk of unauthorized access to confidential information and exfiltration of the data from insiders</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td><strong>Stable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Risk of unauthorized access to confidential information from unauthorized network device changes</td>
<td>High</td>
<td>Elevated</td>
</tr>
<tr>
<td>12. Risk of unauthorized access to confidential information from external attackers</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>14. Risk of unauthorized access to confidential information from a network breach</td>
<td>High</td>
<td>Elevated</td>
</tr>
<tr>
<td>15. Risk of unauthorized access to confidential information from wireless devices</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>16. Risk of unauthorized access to confidential information from inactive system and application accounts</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>18. Risk that in-house developed software has cyber security control gaps</td>
<td>High</td>
<td>Elevated</td>
</tr>
<tr>
<td>2. Risk of unauthorized access to confidential information from unauthorized and unmanaged software</td>
<td>High</td>
<td>Elevated</td>
</tr>
<tr>
<td>3. Risk of unauthorized access to confidential information from unmanaged hardware and software configurations</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>7. Risk of unauthorized access to confidential information from email and web browsers</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>8. Risk of unauthorized access to confidential information from malware</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>9. Risk of unauthorized access to confidential information from network ports</td>
<td>Elevated</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
Each sub-control receives a scored Control Rating. The total scoring equals the overall Control Effectiveness (Assurance Rating).

Inherent Risk + Control Effectiveness = Residual Risk

### CSC Std Control Objective

<table>
<thead>
<tr>
<th>BOTO Control Name</th>
<th>BOTO Control Description</th>
<th>Owner</th>
<th>Frequency</th>
<th>Type</th>
<th>Method</th>
<th>Control Rating</th>
<th>Assurance Rating</th>
<th>Residual Risk</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 1.1 Active and Passive Device Discovery System</td>
<td>Management directed practice barcodes are affixed to new devices at procurement and once added to the network are scanned, inventoried and recorded in Ticketing System.</td>
<td>Dave Shackleford</td>
<td>Ongoing</td>
<td>Preventive</td>
<td>Hybrid</td>
<td>Strong</td>
<td>Strong</td>
<td>Low</td>
<td>Develop Asset Management Standard, and subsequent Procedures.</td>
</tr>
</tbody>
</table>

---

RSAC

Inherent Risk + Control Effectiveness = Residual Risk

RSAC Conference 2018
Benefits To Your Organization

1. The Risk framework is the foundation of your enterprise security strategy.
2. The Risk Dashboard is the core of your security reporting and presentations to the CEOs and Board.
3. Through Interactive dashboards, risks are more tangible for departments.
4. Security becomes a “center of excellence” for risk management.
Key Takeaways

1. Risk should be the cornerstone for your security program.
2. You need business buy-in.
3. How you think about risk is specific to your organization.
4. Keep things simple and interactive.
5. You need frameworks and visualization tooling.
Apply What You Have Learned Today

- Next week you should:
  - Identify team members to form a security risk working group
  - Identify key stakeholders within the different business units/departments

- In the first three months following this presentation you should:
  - Have a BnL listing of all relevant risk scenarios based on initial meetings and feedback from the business
  - Adopt and customize a tailored control framework, at the control objective level

- Within six months you should:
  - Have an initial understanding of your key risks by department, and resulting critical controls
  - Plan to incorporate control audit scores into the risk picture
  - Have an low confidence security strategy/control mitigation plan based on the risks the business has told you are most critical to mitigate
Questions

Rick Patterson
rpatterson123@gmail.com

“Excuse me, but is this The Society for Asking Stupid Questions?”