UNDERSTANDING SECURITY FRAMEWORKS AND THE BENEFITS TO YOUR FIRM

Ty Smith and Jason Broz

March 19, 2019

RSM

Agenda

- Introductions
- About the research
- The frameworks
- Why implement
- What to consider when implementing
- How to implement

RSM

About your presenters

Ty Smith
Supervisor – Security, Privacy & Risk Consulting

- RSM National Law Firm Growth and Strategy Team
- Ohio Army National Guard Captain
- Auburn University MBA Candidate (Fall ‘19)
- Associate CISSP, Six Sigma Lean, Change Management Specialist

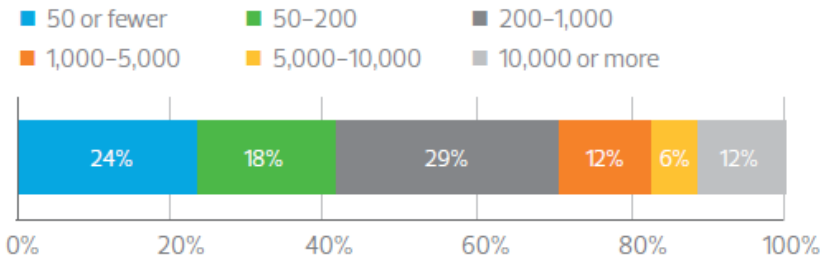
Jason Broz
Manager – Security, Privacy & Risk Consulting

- Certified Information Systems Security Professional (CISSP)
- Payment Card Industry (PCI) Qualified Security Assessor (QSA)
- Certified Information Systems Auditor (CISA)
- Certified Privacy Professional/USA (CIPP/US)
- SANS/GIAC Security Leadership (GSLC)

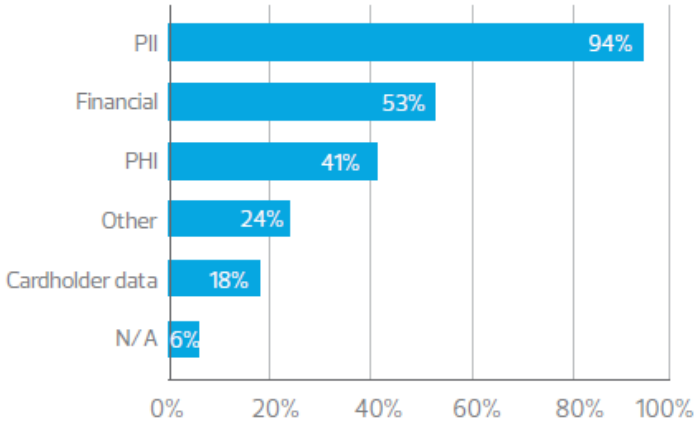
ABOUT THE RESEARCH

Research

Survey participants by number of employees



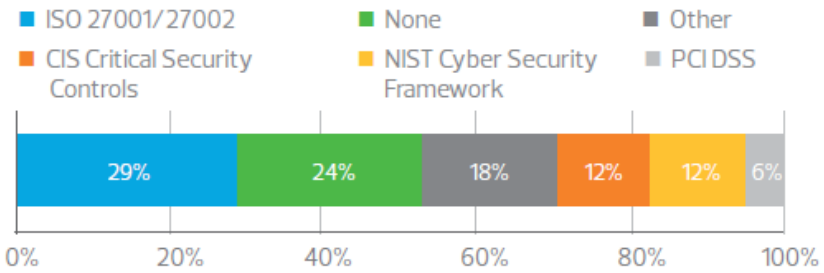
Types of data stored



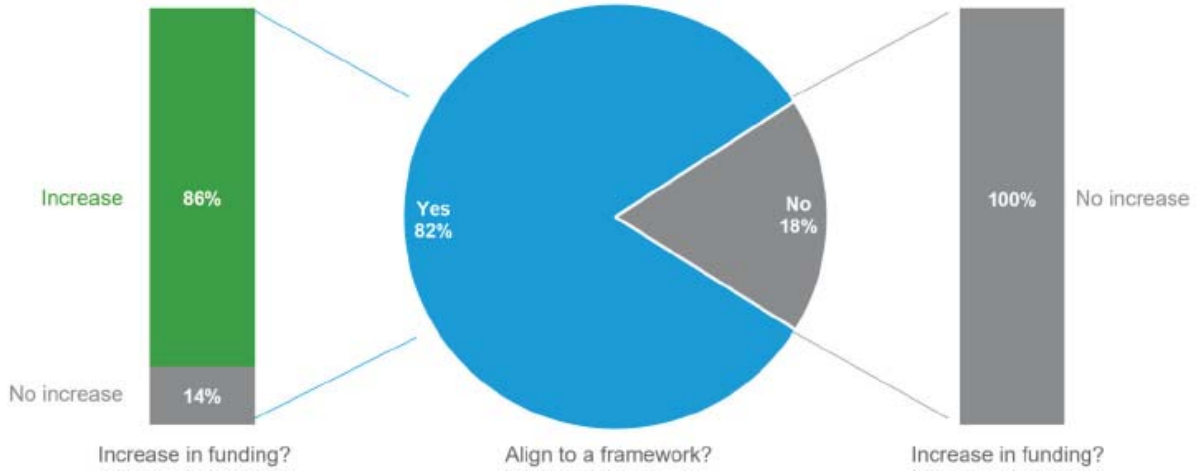
- RSM surveyed firms between January and February of 2018
- A wide variety of firms responded, ranging from under 50 employees to over 10,000
- Nearly all firms store some data, the largest response set being personally identifiable information
- Most firms stored multiple data sets

Survey findings

- Survey respondents indicated several frameworks being used within the industry
- Large firms trended towards ISO
- Almost a quarter of firms responding indicated they did not map to a framework

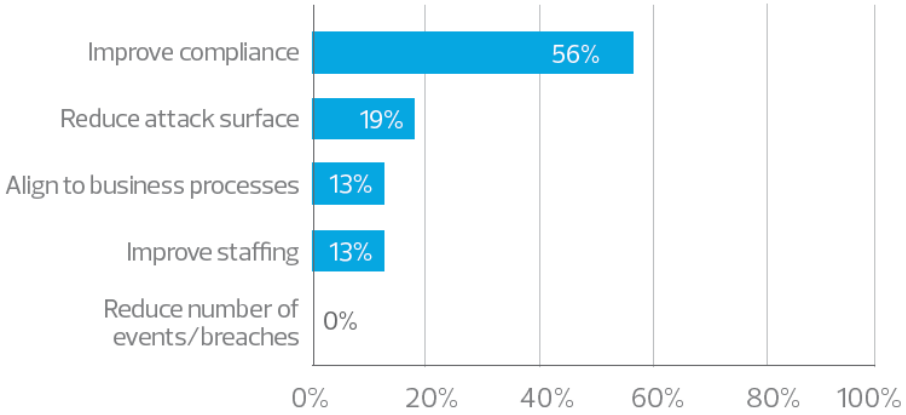


Follow the money



- Of those responding that they do not follow a framework, 100 percent have not received an increase in their security budget in a three year period
- Eighty six percent of those responding they do map to a framework have received an increase in funding

Budget justifications

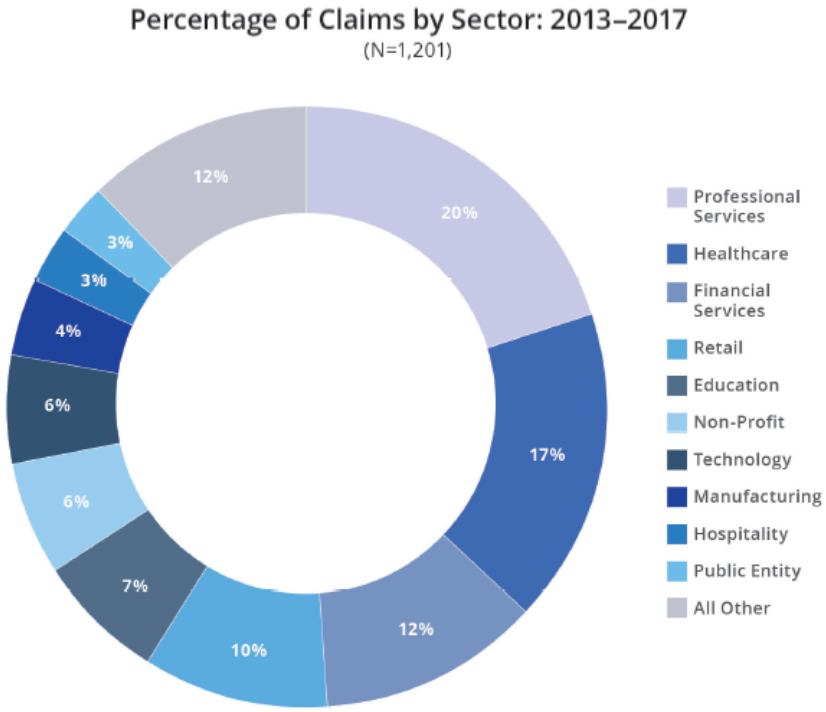


- Improved compliance was the most common justification for firms that saw increases in their budget
  - Aligning your program to a framework can help to make smooth transitions to new compliance objectives
- Frameworks can help reduce the burden on IT staff with standardization

WHY IMPLEMENT

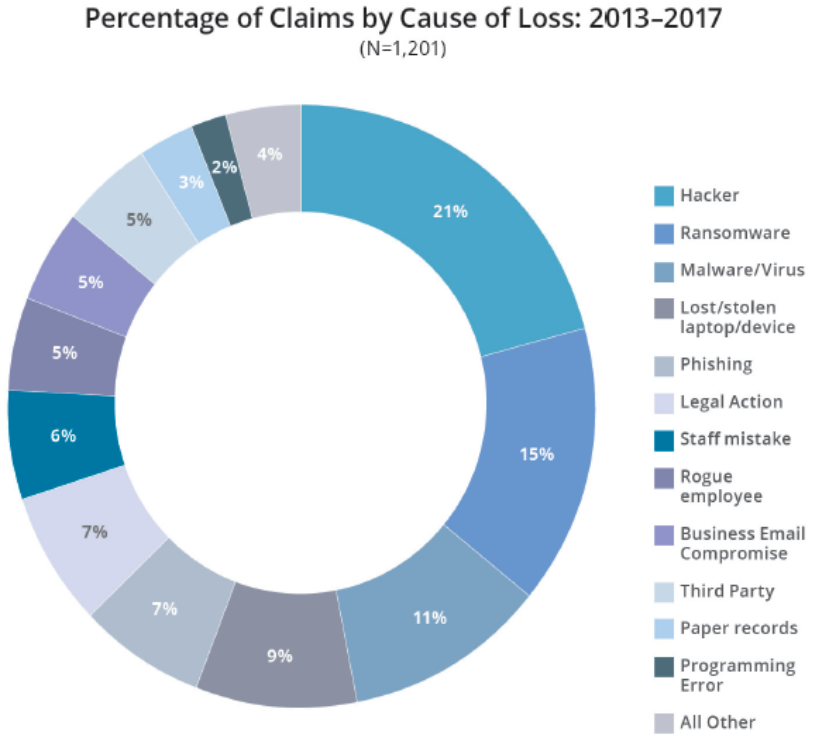
2018 NetDilegence/RSM Cyber Claims study

- 2013-2017 study
- Cyber liability claims
  - Professional services 20% of all claims
  - 263 total claims in professional services
  - Average total cost of a breach in a professional services firm: $168,000
  - Firms accounted for 3% of total aggregated breach cost



2018 NetDilegence/RSM Cyber Claims study

- Cause of loss
  - Hackers 21%
  - Malware/virus 11%
  - Phishing 7%
  - Legal action 7%
  - Business email 5%
  - Programming error 2%
- Law firms had the highest compromise rate (60%) during RSM's testing in 2017
- Losses could have been minimized through a managed security program



THE FRAMEWORKS

ISO 27001

- The largest percentage (29%) of respondents align to ISO 27001
  - Best for large firms
  - 80% of ISO 27001 respondents have over 1000 employees
  - All firms who align to ISO 27001 saw an increase in their security budget
  - 2/5 of ISO 27001 respondents saw an average increase in security budget between 11% and 20%
- The cost
  - Only 1500 organizations have gone through the certifications process
  - Most firms aligning to the framework allocate over $100k to the process

ISO AT A GLANCE

- Aligned with GDPR
- Focused on process and documentation
- Lack of technical detail
- Higher cost to implement
- Best fit for large or international firms

RSM

NIST Cybersecurity Framework (CSF)

- Developed and released by the US Government in 2014
- Only 12% of respondents align to the CSF
  - Saw the largest increase in funding on average (20%)
- Guidelines provided are flexible
  - The flexibility allows for implementation across a wide variety of industries
  - Should be used by established programs
- Best choice for US middle-market firms

NIST CSF AT A GLANCE

- Increasing in popularity
- Required for government agencies and some private partners
- More ambiguous and harder to implement
- Fewer resources available
- Best fit for established cybersecurity programs that work with federal organizations or government contractors

RSM

Center for Internet Security (CIS)

- 18% of middle market firms responded that they map to CIS
  - Largest increase in overall funding over three years
- Technical focus with limited documentation
  - Firms can supplement small IT teams with technology
  - Governance support is needed from CISO
- Best for small to middle market firms without established programs

CIS AT A GLANCE

- Correlates with increased funding
- Strong technical focus
- Lack of guidance on process and program level
- Difficult to implement without support
- Best fit for firms with limited budgets

RSM

Payment Card Industry Data Security Standard

- Developed by credit card brands in 2004
  - Significant guidance and documentation available
- Only 9% of firms respondents follow the PCI DSS
- Clear and concise guidance provided by the framework
  - Technical control implementation
  - Governance structure
- PCI does not have to apply only to credit card information; framework can be modified for all sensitive data

PCI DSS AT A GLANCE

- Globally recognized, trusted, well-established
- Comprehensive and easy to implement
- Aligns with other frameworks (NIST CSF)
- Adaptable to different sensitive data sets besides cardholder data
- Best fit for most firms

RSM

WHAT TO CONSIDER

When implementing a framework

Selecting a framework

- Even if your firm is already using a framework, may not mean it is the right one
  - You can use a hammer to dig a hole, but a shovel is a lot more efficient
  - The wrong framework can drain internal resources, frustrate overworked employees, and possibly make your organization less secure
- Each framework has a particular purpose and function
  - Use frameworks to your advantage
  - Understand how to make frameworks flexible to work with business process

RSM

Identifying key data

- 94% of firms store some type of sensitive or confidential data
- Different types of data have regulatory requirements that may help to define a framework (HIPAA, PCI, etc.)
- If your data is not regulated, there may still be client requirements that are placed on your firm through contracts or agreements

RSM

Assessing client needs

- Most law firms RSM advises are dealing with client requirements from one or multiple clients
- Requirements range from conducting penetration test and vulnerability scanning to naming a CISO and quarterly reports to the Board or Partner team
- Firms must holistically look at the requirements placed on them from all of their clients to see which framework best fits their situation
- The right framework can help efficiently cover requirements and provide a return on investment to partner teams

RSM

Evaluate effectiveness

- A successful framework is not just a set of guidelines that meets client requirements and “Checks the box”
- Frameworks should be judged on their ability to secure data efficiently and effectively
- Firms should determine metrics to ensure their framework is implemented properly
  - Events stopped, patching timeframes, strengthened baselines, etc.
- Frameworks should work with firm leadership to determine effectiveness and efficiency

RSM

Plan towards future goals

- As your firm continues to expand and grow, business leaders should be involved with the choice of framework to incorporate future plans
  - For example, if the firm is looking to work internationally in the coming years, then ISO 27001 might be the best framework
- With so many choices out there, it is important to invest in a framework that not only works today, but can be scalable enough to grow with your firm

RSM

HOW TO IMPLEMENT

Frameworks

- As law firms become a bigger target for cyber criminals, properly securing data will become even more important
- Implementing a framework will help to secure your clients' data
- No matter what framework your firm chooses, these steps will help to ensure that it is implemented properly

RSM

Roadmap

1. Establish a governance structure
   - Select a program owner to oversee implementation and data owners to help with security decisions
2. Perform data discovery
   - Determine where data is stored, processed, accessed, and who it is transmitted to within the firm's environment
   - Document data flow diagrams
3. Classify Assets
   - Determine which assets are critical to the firm based on how data flows throughout the environment

RSM

Roadmap

4. Conduct a risk assessment
   - Identify, analyze, and document organizational risks
   - Prioritize plans for remediation towards an acceptable level of risk for the firm
5. Apply controls
   - Use the risk analysis and framework to identify missing controls and apply them within the environment
6. Develop security processes
   - Create consistent, repeatable processes around patch and vulnerability management, device hardening, etc.
7. Review program regularly
   - Continually improve your program by reassessing yearly during your risk assessment process

RSM

THANK YOU FOR YOUR TIME AND ATTENTION

RSM US LLP

23340 Miles Road
Cleveland, Ohio
216 927 8200

+1 800 274 3978
rsmus.com

RSM