RIGIDBITS

Cybersecurity – How to Prevent an Attack and Mitigate Your Risk

Security ▪ Compliance ▪ Open Discussion

Flood & Peterson

Prepared for Alliance Summit–
September 2021

Greg King

RISK ADVISOR

Greg King has been with Flood and Peterson since 2019 and he has over 7 years of experience in the insurance industry. He is passionate about leveraging his legal and business knowledge to create personalized risk solutions. Greg's specialties include Education, Directors & Officers (D&O), Healthcare, Manufacturing, Non-Profit, Technology and other miscellaneous classes.

Greg received his J.D.in 2010 from Michigan State University College of Law with a focus on business/corporate law.

Contact information

Email
Phone: 720.977.6030
Cell: 720.822.7219

Sean Gingerich

RISK ADVISOR

Sean Gingerich joined Flood and Peterson in 2004 and serves as a Risk Advisor. He has nearly 20 years of insurance industry experience. He is strategic in the management and marketing of large client accounts, while building and maintaining business relationships. Through his experience, he has developed a wide array of skills and knowledge in risk management, surety, and business consulting. Sean is well versed in the exposures clients face from a variety of industries, including Commercial, Construction, Manufacturing, Transportation, and Environmental.

Sean received a Bachelor of Science degree in Business Administration from the University of Redlands. He maintains his Commercial Lines Coverage Specialist (CLCS) designation.

Contact information

Email
Phone: 970.506.3205
Cell: 970.371.7705

Flood & Peterson

Presenter

- Identify and Reduce Cybersecurity Risks
- Test and Re-enforce Security Controls
- Develop and Implement Cybersecurity Programs
- Align with Regulations and Best Practices
- Investigate and Recover from Cybersecurity Incidents
- Serve Independent Agencies through Education and Awareness

RIGIDBITS

Cybersecurity Professional Services and Consulting | Digital Forensics and Incident Response

Presenter

- Background in Mathematics, Education, and Sales
- Mathematics, BA (2006 - University of Colorado at Boulder)
- Focus on Customer Education and Problem Solving
- Technology experience in Education and Business fields
- 4 years advising businesses on cybersecurity related goals

Ryan Smith

Director of Sales and Customer Success | Rigid Bits, LLC

Agenda

1. Cyber 101
2. IT vs Cybersecurity
3. Cybersecurity for CCB's and PASA's
4. Where to Begin
5. Cyber Liability
6. Resources
7. Q&A

Objectives

1. Understand a risk-based approach to cybersecurity
2. Learn how to break down your cybersecurity risks
3. Identify common requirements and best practices
4. Walk away with a few next steps to improve your protections

What this is all for...

- Protection of the organization
  - Keeping operations and business moving
  - Avoiding unnecessary costs
  - Maintaining reputations and relationships

- Protection of those that rely on you
  - Families that are already going through difficult challenges
  - Children and their high-risk data

Cybersecurity 101

“There is no secure. There is only more or less risk.”

Cybersecurity 101

- Risk = Likelihood x Impact
- Vulnerability
- C.I.A. = Confidentiality, Integrity, Availability
- Identify, Mitigate and Reduce Risk Exposure

Cybersecurity 101

- Risk = **Likelihood** x Impact
- Vulnerability

- C.I.A. = Confidentiality, Integrity, Availability
- Identify, Mitigate and Reduce Risk Exposure

Ease of discovery
How easy is it for this group of threat agents to discover this vulnerability?

Ease of exploit
How easy is it for this group of threat agents to exploit this vulnerability?

Awareness
How well known is this vulnerability to this group of threat agents?

Intrusion detection
How likely is an exploit to be detected?

Cybersecurity 101

- Risk = Likelihood x **Impact**
- Vulnerability
- C.I.A. = Confidentiality, Integrity, Availability
- Identify, Mitigate and Reduce Risk Exposure

C.I.A.

Specific cybersecurity impacts to your **systems** and **data**

Additional Impacts

Loss of customer trust

Regulatory fines/penalties

Financial impact

Cybersecurity 101

- Risk = Likelihood x Impact
- Vulnerability
- C.I.A. = Confidentiality, Integrity, Availability
- Identify, Mitigate and Reduce Risk Exposure

Efficiency and convenience comes with a cost of associated technological risk.

Making cybersecurity decisions based on fear reflects an attempt to eliminate risk.

There is no way to completely remove all elements of risk.

Risk Vs. Secure

RISK

- Quantifiable/Qualifiable
- Range of possibilities
- Considers likelihood and impact
- Clear, concise, and actionable
- Leads to proper decision making

SECURE

- Limited in quantification, no qualification
- Binary Yes or No
- Alludes to likelihood, ignores impact
- False clarity, unrealized risks
- Leads to improper decision making

Problems That Arise

- Unrealized risks are more likely to be present, no way to compare known risks, and mis-prioritization of efforts and budget
- Missing best practices, not in compliance, unable to demonstrate Due Diligence & Due Care, and possibly at risk of fines
- Underestimating potential impact of an incident, unprepared for appropriate response efforts, and not financially prepared for immediate or long-term cost

IT vs Cybersecurity

IT vs. Cyber Goals

- Operational support
- System up-time
- Access to email and resources
- Hardware troubleshooting
- Asset management
- Telephony and communications

IT

- Identify and mitigate risks
- Compliance support efforts
- Identification of vulnerabilities
- Planning and tracking of cybersecurity best practices
- Incident Recovery Efforts

Cybersecurity

Cyber Certifications and Associations

- GPEN | GIAC Penetration Tester
- OSWP | Offensive Security Wireless Professional
- CISSP | Certified Information Systems Security Professional
- EnCE | EnCase Certified Examiner
- GCFA | GIAC Certified Forensic Analyst
- A+ | Computer Software and Hardware
- Security+ | CompTIA Security

- (ISC)² | International Information System Security Certification Consortium
- ISSA | Information Systems Security Association - Denver Chapter
- Longmont Chamber of Commerce
- Colorado Technology Association
- Independent Insurance Agencies of Texas (IIAT)
- Professional Independent Insurance Agents of Colorado (PIIAC)
- Agents Council for Technology (ACT)
- GIAC Advisory Board

Combined IT & Cybersecurity

What goes wrong?

- ✗ Marketing demands force the use of buzzwords
- ✗ Conflict of interests
- ✗ Missing certifications, credentials, and capabilities
- ✗ Focus on security products instead of prioritizing risks
- ✗ Attempt to buy the way out of risk
- ✗ IT providers are prime targets for 3rd party attacks due to their access
- ✗ Assumption that IT is adequately addressing cybersecurity concerns
- ✗ Jack of all trades, master of none

Cybersecurity for CCB's and PASA's

Risks for CCB's and PASA's

Key areas of risks to be aware of:

- Ransomware Attacks
- Phishing Attacks
- Business Email Compromise
- Risks in your environment
  - People
  - Public-facing assets
  - Internal:
    - Information Systems
    - Databases
    - Methods of interacting with secure tools and data
- 3rd Party Risks
  - Cloud technology
  - Integrations
  - Other Vendors

Requirements for CCB's and PASA's

Key regulations:

- State Laws
  - Data Security
  - Breach Notification
  - Data Disposal
- Federal
  - HIPAA
- 3rd Party Data Security Requirements
  - Contracts
  - Data Security Addendums
- Insurance
  - Cyber Liability minimum requirements

Addressing Risks and Requirements

Common Terms and Approach:

- Contract/legal language
- Identifying “Recommended” cybersecurity controls vs “Required”
- It’s not one size fits all
- Approaches:
  - “Take reasonable measures to protect non-public information”
  - “Risk Based Approach”
- Key Terms:
  - NPI, PII, PHI, etc
  - WISP, ISP, Sec Prog Plan

Addressing Risks and Requirements

Common Patterns in Cybersecurity Program and Structure:

- Risk Assessment
- Incident Response Plan
- Policies & Procedures
- Security Program Plan

Addressing Risks and Requirements

Common Patterns in Cybersecurity Program and Structure:

- Cybersecurity Frameworks
  - Best practices and standardizations
  - National Institute of Standards and Technology (NIST)
  - Center for Internet Security (CIS Controls)
- Leveraging Frameworks
  - Gives you ability to choose what you're doing or not doing
  - Allows for an explanation of "why"
- Regulations
  - These typically follow the recommendations from frameworks and best practices
  - Most risk reducing controls are pulled out and specified (like MFA)
  - Some regulations acknowledge others
    - Ex: A law or 3rd party requirement may be satisfied if HIPAA requirements are met

Where to Begin

Risk-Based Cybersecurity with Rigid Bits

Start with understanding your risk

- Identify known risks and seek out unknown risks – get it all out in front of you
- Score and rank risks based on their Likelihood and Impact so you can compare effectively
- Leverage this insight in decision making steps to prioritize addressing risks, budget, time, and effort

Risk-Based Cybersecurity with Rigid Bits

Start with understanding your risk

- Conduct a Risk Assessment
- Scan for Vulnerabilities
- Conduct a Penetration Test

Risk-Based Cybersecurity with Rigid Bits

Prepare for potential incidents

- Based on risk, consider how an attack may unfold and have pre-defined steps to follow
- Align with your breach notification requirements
- Minimize the time to identify and respond to breaches to bring down the potential cost
- Test the effectiveness of your plan and make sure roles/responsibilities are defined and no gaps exist

Risk-Based Cybersecurity with Rigid Bits

Prepare for potential incidents

- Develop and Implement an Incident Response Plan
- Build a relationship with a team that offers Forensics services and knows your environment
- Implement tools to make response faster and more effective

Risk-Based Cybersecurity with Rigid Bits

Begin mitigating risks with best practices

- Based on risk, leverage a cybersecurity framework or best practices to guide risk reduction
- Demonstrate your Due Diligence and Due Care by documenting the “what and how” of your approach
- Show how compliance requirements are being met

Risk-Based Cybersecurity with Rigid Bits

Begin mitigating risks with best practices

- Write and Implement Policies & Procedures
- Get guidance on impactful steps to take in risk reducing practices
- Train staff and conduct regular phishing simulations
- Monitor for stolen credentials

Risk-Based Cybersecurity with Rigid Bits

Continue progress and address gaps

- Build a recursive cybersecurity program that adapts and grows as you continue
- Reassess your status and direction annually or after major changes to processes or systems
- As progress is made, keep momentum by implementing defense-in-depth and diving deeper into risks and related protections

Risk-Based Cybersecurity with Rigid Bits

Continue progress and address gaps

- Ongoing consulting engagements that evolve as you go
- Implement Enhanced Email Security Tools
- Get guidance when considering advanced cybersecurity tools like EDR and SOC solutions

Cyber Liability Insurance

Cyber Liability Insurance – The Policy

- Not all policies are created equal
- Coverage
  - Third-Party
  - First-Party
- Resources

Cyber Liability Insurance – The Policy

Third-Party

- Multimedia Liability
- Security & Privacy Liability
- Privacy Regulatory Defense and Expense
- Bodily Injury
- Property Damage

Cyber Liability Insurance – The Policy

First-Party

- Breach Event Cost
- Business Income
- Contingent BI
- Post Breach Remediation
- Reputation/Brand
- System Failure
- Dependent System Failure
- Cyber Extortion
- Cyber Crime
- Bricking
- Property Damage Loss
- Reward Expense
- Court Appearance Cost

Cyber Liability Insurance – The Policy

Resources

- Legal
- Forensic
- Crisis management

Staying Insurable

- Multi-factor Authentication
  - Email
  - All remote connections to network
- Security Awareness Training
  - Phishing
  - Ransomware
- Backups
  - Stored off-line (not accessible from local network)
  - Testing ability to restore backup
- Risk Advisor

Resources

Where to start

1. Visit “rigidbits.com”
    - Get recommendations and access to resources
        - Free downloads, guides, blog posts, and webinars
        - Plan of Action & Milestones (POA&M)
        - Quick Risk Questionnaire
        - HIPAA Checklist
        - Sign up for our Newsletter

2. Schedule your free Cybersecurity Risk Consultation
    - Learn about your immediate risks and compliance gaps
    - Get ideas about simple ways to improve your risk
    - Explore guidance on how to build and grow a sustainable cyber program

3. Send us your questions
    - info@rigidbits.com
    - (800) 626-5056

October – Cybersecurity Awareness Month

Free events and resources from Rigid Bits:

- Events and resources to help overcome cybersecurity and compliance challenges
- Learn about ways to reduce cybersecurity risks and build a stronger cybersecurity culture
- Boost your cyber-knowledge over short, weekly webinars
- Sit in on weekly guest webinars in a wide variety of topics
- Participate all month-long for a chance to win $100 and other giveaways
- Join our all-access pass to follow along:
  https://rigidbits.com/october-2021-cybersecurity-awareness-month/

Questions?

info@rigidbits.com

(800) 626-5056