Information Security Risk Management

ABOVE SECURITY™
DEPUIS/SINCE 1999

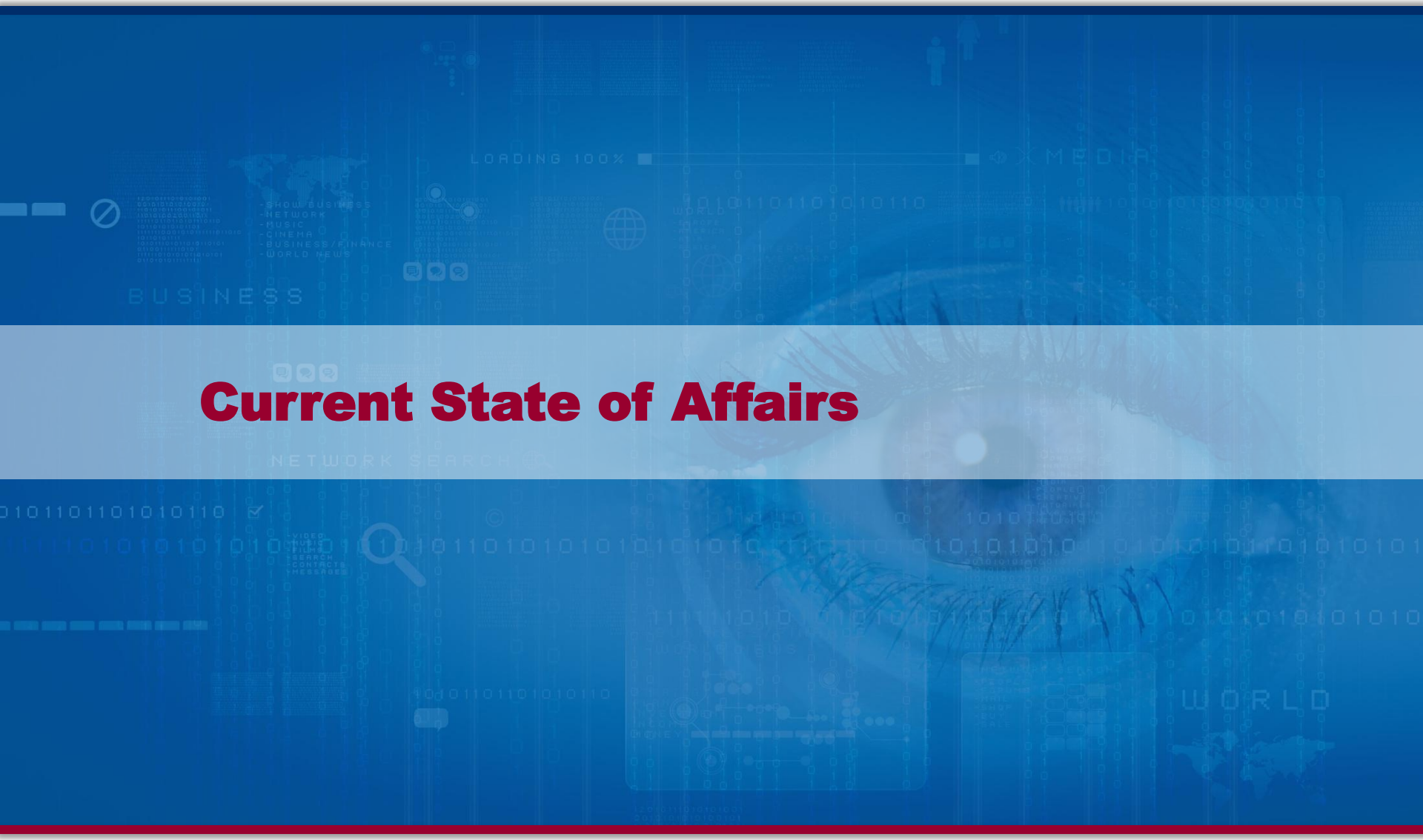
June 11, 2013

Patrick Perreault
Daniel Gaudreau

Agenda

- Current State of Affairs
- Why Information Security?
- The Role of Risk Management
- Information Security Threats, Controls and Performance Measures
- Conclusion

Current State of Affairs



In the News

Threat of the Week: DDoS Becoming an Expensive Fact of Life

BY ROBERT MCGARVEY
March 4, 2013 • Reprints

MSUFCU Warns of Phishing Scam

By Fox 47 News
CREATED JUN. 8, 2013

Kingsport credit union hit by fraud

By Kyle Benjamin, kbenjamin@wcyb.com

POSTED: 6:09 PM May 31 2013 | UPDATED: 12:00 AM May 31 2013

Threat of the Week: Mayhem in the Mobile Browser

BY ROBERT MCGARVEY
June 4, 2013 • Reprints

5 Tips for Protecting Against DDoS Attacks

BY PHIL LERNER
March 13, 2013 • Reprints

How to Succeed When Your Defenses Fail

BY ERIC BROWNING
January 14, 2013 • Reprints

NAFCU's Berger advocates measures to help credit unions address cybersecurity

Published on **May 22, 2013** by **Sarah Jackson**

Nervous Credit Unions Seek Buffers After DDoS Attacks

BY ROBERT MCGARVEY
February 20, 2013 • Reprints

Time to Protect Yourself From State-Sponsored Attacks

BY CALUM MACLEOD
March 4, 2013 • Reprints

Credit Union's State of Mind

- **"We are not the targets"**: Credit unions have the impression that larger banks are more likely to be victims of a cyberattack.

  While this may be true when *hacktivism* is concerned, it does not take other attack motivations into account.

- **Shame**: Everyone is reluctant to expose weaknesses.

  Putting your head in the sand will not make the problem go away...

- **Confusion**: Why do I need security? Where do I start? What is my current situation? What are my priorities?

  A risk management-based approach will enable you to define your needs and help you structure your efforts.

Why Information Security?

ABOVE SECURITY™
DEPUIS/SINCE 1999

Information Security

Why should credit unions consider improving their security footprint and monitoring?

- Your business increasingly depends on information technology and, therefore, is more prone to damage through technological means:
  - Internet banking
  - Internet marketing
  - Network connections to partners and suppliers
  - What percentage of your employees work with a computer?
- Openness to the world and increased reliance on technology creates new business opportunities, but also introduces new risks that have to be identified and measured.

Information Security

Why should credit unions consider improving their security footprint and monitoring?

- Laws, regulations and standards are imposed on you and noncompliance could result in monetary loss (and, in some cases, imprisonment)
  - Bank Secrecy Act (BSA)
  - Sarbanes-Oxley Act (SOX)
  - U.S. State Security Breach Notification Laws
  - Gramm-Leach-Bliley Financial Modernization Act (GLBA)
  - Payment Card Industry's Data Security Standard (PCI-DSS)

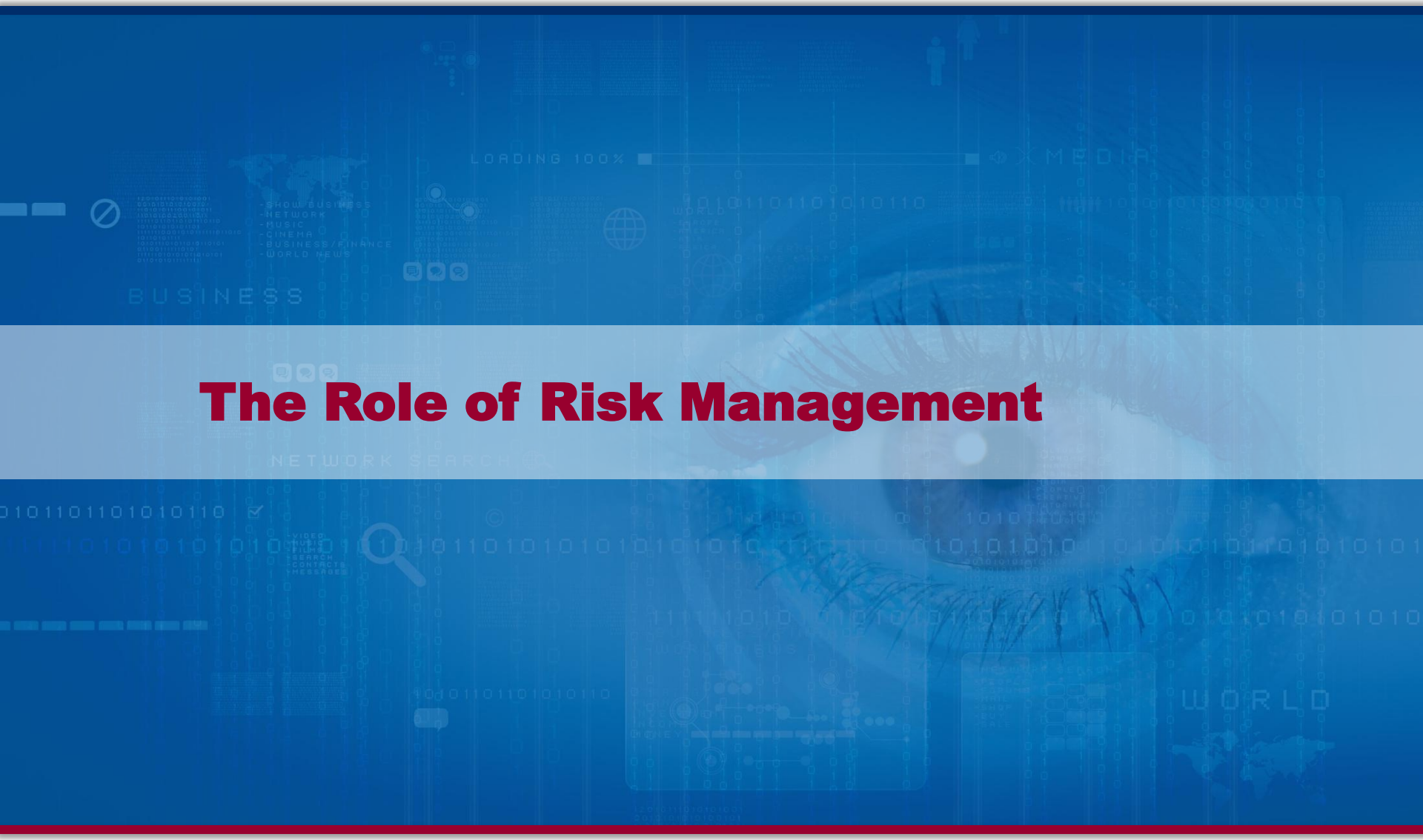
Information Security

Why should credit unions consider improving their security footprint and monitoring?

- The value of a security program comes down to costs versus benefits:
  - Compliance to laws, standards, regulations…
  - Competitive advantage
  - Business catalyst
  - **Risk management**
- Security is about:
  - Confidentiality
  - Integrity
  - Availability

Risk management is about finding, measuring, controlling and monitoring the risks to confidentiality, integrity and availability.

The Role of Risk Management

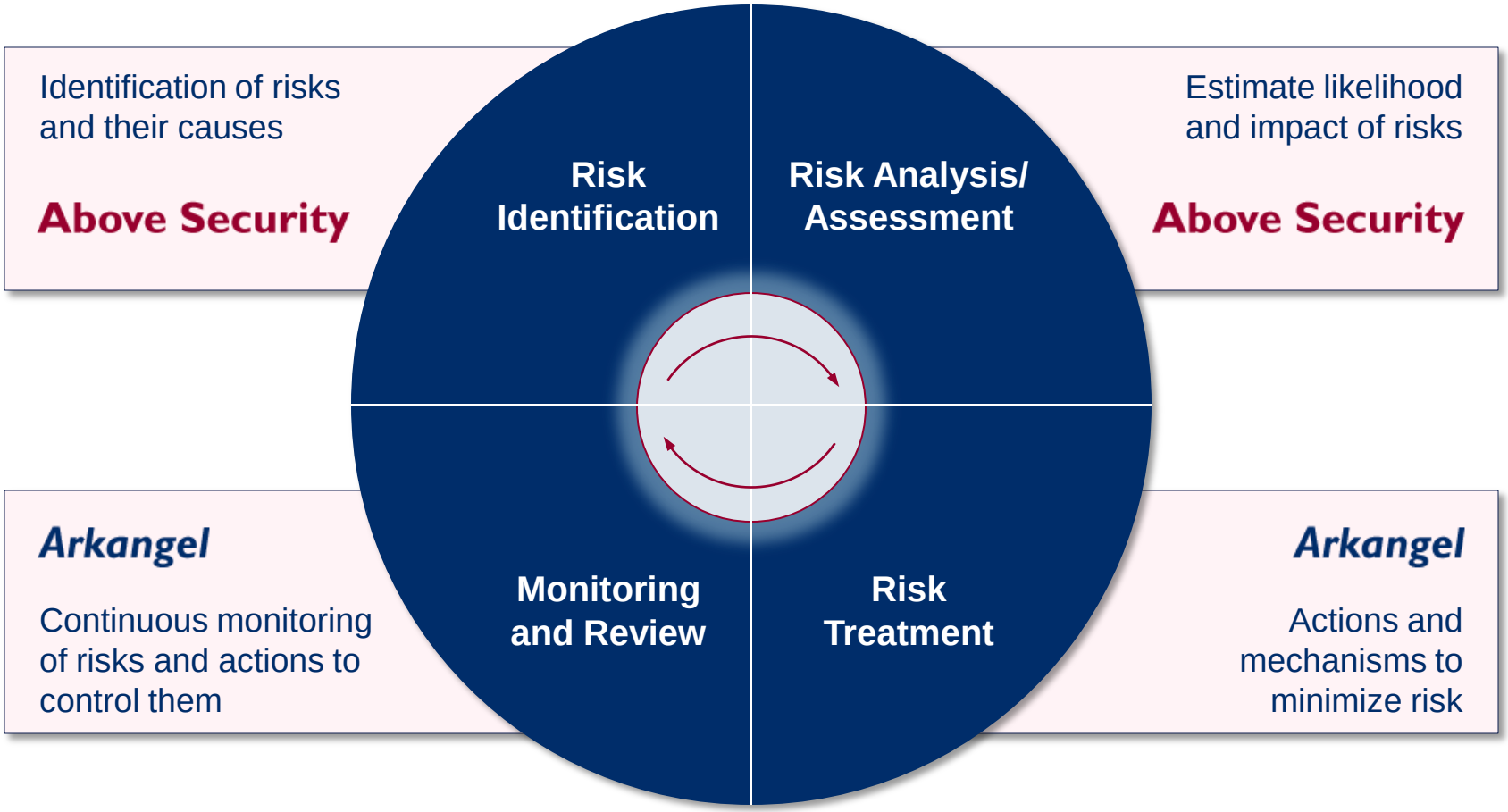


ABOVE SECURITY™
DEPUIS/SINCE 1999

Risk Management

- Credit unions likely dedicate much time and effort to organization-wide risk governance and oversight relating to:
  - Legal
  - Health and safety
  - Financial
  - Governance
- Loss of data/theft of information, vulnerability to cyberattacks and the myriad of related IT security threats need to be considered equally when determining potential business risks and developing mitigation strategies

Risk Management



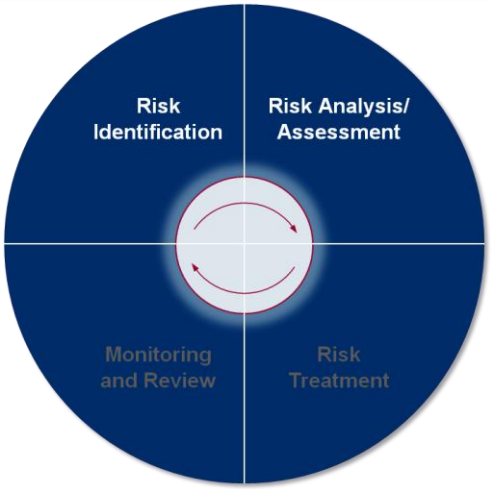
Risk Management

An **analysis of the information security risks** is necessary:

- As part of an overall business risk management effort
- At least annually and any time security incidents occur
- As part of an information security management program
  - Risk Management Framework (NIST)
  - Carnegie Mellon's OCTAVE® (Operationally Critical Threat, Asset and Vulnerability Evaluation℠) is a suite of tools, techniques and methods for risk-based information security strategic assessment and planning
  - ISO 27001 Information Security Management System
  - PCI Data Security Standard (req. 12.1.2)

Risk Management

Risk identification and measurement



- With the participation of:
  - Executives (long-term visibility into business strategy)
  - Owners of information assets (who better to evaluate value?)
  - IT security professionals (best practice, experience)
- Risk can be measured as a function of four factors:
  - A = The value of the assets
  - T = The likelihood of the threat
  - V = The nature of the vulnerability, i.e. the chance that it can be exploited (proportional to the potential benefit for the attacker and inversely proportional to the cost of exploitation)
  - I = The probable impact, i.e. the extent of the harm

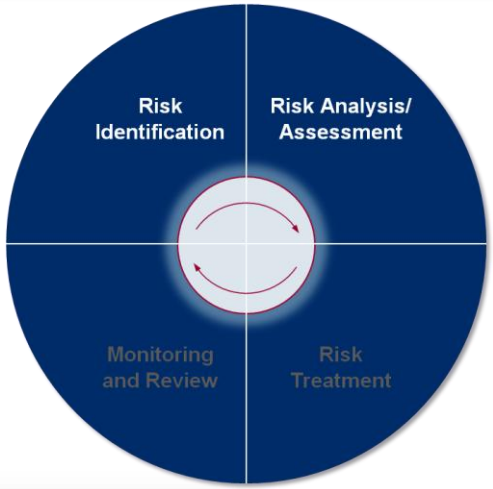
Risk Management

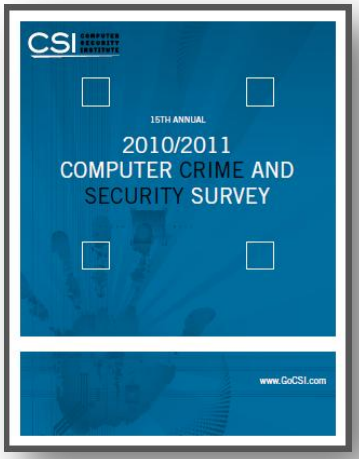
Risk identification and measurement

- Get inspiration from multiple sources to identify risks and prioritize your security needs inline with:
  - Contracts with clients and partners
  - Standards, laws and regulations of your industry
  - Past experiences
  - Supplier white papers
  - Industry opinions (Gartner, Forrester, CSI, etc.)

CAUTION Their goal is to showcase their product!

  - They are not very comprehensive
  - They may not be applicable to your industry
  - They may already be obsolete





ABOVE SECURITY™ DEPUIS/SINCE 1999

Risk Management

Risk treatment methods

- Avoid (eliminate)
- Control/reduce (optimize, mitigate)
  - Layered controls are the best approach to optimal information security
- Transfer/share (outsource, insure)
- Accept (retain and budget)

Above Security

Risk Management

Monitoring and review

- Often neglected... the perception is that security solutions resolve the issues... they are installed and then forgotten.
- Do you have the proper resources, expertise, procedures and tools in place to monitor your controls?
- Do you have the proper procedures and tools in place to measure control performance?

Managed Security Monitoring for Maximum ROI

- Centralized management of logs and alerts produced
- 24/7 monitoring and response

Risk Management

Monitoring and review

Managed Security Monitoring for Maximum ROI

- Trained and dedicated experts
- Conformity to standards (PCI)
- Measure the controls' (effectiveness, efficiency, constraints)
- Provide reports contributing to risk management efforts
  - Continuous improvement
  - Non biased observations and recommendations
- Participates actively in Computer Incident Response
  - Planning
  - Detection
  - Response

Information Security Threats, Controls and Performance Measures

ABOVE SECURITY™
DEPUIS/SINCE 1999

Information Security Threats

What threats cast a shadow on credit unions?

- Denial of service attacks (loss of revenue stream)
- Data loss/theft (fines, legal fees, criminal prosecution)
- Service infrastructure damage (loss of productivity)
- Defacement (reputation)

Information Security Controls

What controls are used to address the threats?

- Intrusion Detection Systems
- Anti-DDoS service or device
- File integrity monitoring
- Vulnerability scanning
- Anti-Spam
- Anti-Virus
- Firewalls

There is no *Holy Grail*. Dedicated and layered controls are the best approach to optimal information security. As controls are accumulating, so is the effort to configure, maintain and monitor them!

Performance Measures

Steps to measuring the performance of controls

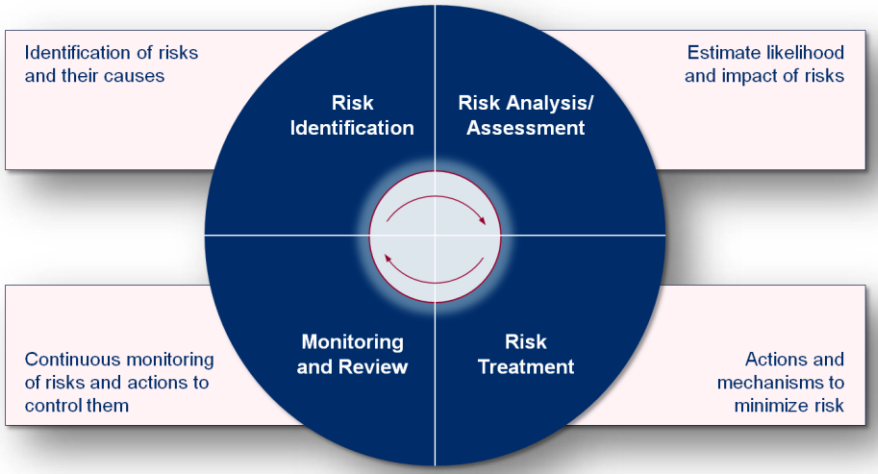
1. Start by clearly identifying the security controls currently in place:
   - Security policy
   - Anti spam
   - Anti virus
   - IDS
   - SIEM
   - Vulnerability scanner
2. Identify the risk that they treat:
   - Loss of productivity
   - Data theft
   - Reputation

Performance Measures (continued)

3. Identify the performance measure(s):
   - Make an effort to align yourself with business controls
   - Internal/external intrusion test
   - Email monitoring
   - Internet usage monitoring
   - External/internal audit
   - Social engineering
   - Volume and type of support requests
   - Volume and type of incidents
   - Knowledge testing (policy, awareness program)
4. Set the frequency
5. Management reports

Conclusion

- Make risk management a priority
  - Identify
  - Evaluate
  - Manage
  - Measure
- Involve all departments
  - Legal: Risks associated with laws
  - HR: Cost of a resource
  - Sales, Marketing, IT, etc.
  - Information security literature and professionals



Raise awareness and involve the executives

Questions?

Daniel Gaudreau CISA, CISM, CISSP, PCI QSA
Executive Vice President of Corporate Affairs
daniel.gaudreau@abovesecurity.com

Patrick Perreault CISM, PCI-QSA
Director of Customer Care
patrick.perreault@abovesecurity.com

ABOVE SECURITY™
DEPUIS/SINCE 1999

Thank You

ABOVE SECURITY™
DEPUIS/SINCE 1999