MOSSADAMS

When Worlds Collide

Improving IT Audit Effectiveness with IT Security

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.

Presenter

Mark Edwards
Director, IT Security
Moss Adams

Today's Impact

Following today's session, you will be able to:

1. Improve the relationship between compliance and security

2. Employ best practices for working with IT security functional teams

3. Identify the most effective use of audit resources for reducing the likelihood of a security breach and accompanying financial loss

4. Discuss key techniques that bad actors, both internal and external, use to compromise systems

Improving the Relationship

Factors Affecting Relationship with IT Security

- Perceived role of internal audit
  - POLICE OR ADVISOR?
- Auditor's knowledge level
  - HIGHLY TECHNICAL OR NON-TECHNICAL ASSESSOR?
- Frequency of audit reviews
  - LESS FREQUENT HIGH QUALITY REVIEWS OR MORE FREQUENT LOW QUALITY REVIEWS?
- Perceived value from internal audit
  - GOOD RELATIONSHIPS IMPROVE PERCEPTION

How to Improve IT Audit & CISO Relationship

- **Empathize.** By understanding the challenges facing the CISO, you are better able to identify opportunities for improvement.
- **Communicate.** Reframing messaging to convey that the role of IT audit is to improve overall security, not police it, subtly alters the dynamic.
- **Grow.** By increasing knowledge of key risks based on industry, sector, size, geography, etc. your value to the organization also increases.
- **Share.** In environments with limited resources, knowledge sharing is invaluable.
- **Collaborate.** Through collaboration, you earn respect and improve your organization's security posture.

Empathize - Understand CISO Challenges

Common challenges facing the CISO:

- Responsibility for information security and strategy
- Executive communications
- Budget, typically underfunded and understaffed
- Plethora of solutions and sales reps
- One breach away from unemployment

Communicate

- Acknowledge role of Audit as assessor and evaluator
- Audit and IT Security have common mission to protect the enterprise
- Findings should not be viewed as bad
- Announce IT audit schedule early to allow sufficient time for IT security personnel to prepare

Grow What You Know About IT Security

- Acquire certification
  - CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA), AT MINIMUM
- Enroll in security trainings
- Subscribe to daily news feeds
- Read annual breach reports
- Understand the IT security risks specific to your company and industry
  - DEVELOP MITIGATING CONTROLS
  - MONITOR CONTROLS

Share What You Know About IT Security

- Become the IT Security Subject Matter Expert (SME) for Audit
- Share relevant IT security news and developments with peers

Collaborate

- Ask IT Security how you can improve the audit experience
- Emphasize that Audit and Security are partners; the goal is to prevent security breaches
- Join committees or communities related to IT security

Working with IT Security Teams

IT Auditor Preparedness

- Research relevant IT security issues prior to audit
  - SUBSCRIBE TO AND READ IT SECURITY BLOGS
  - READ BREACH & THREAT REPORTS, ESPECIALLY YOUR INDUSTRY/SECTOR:
    - Verizon, Cisco, FireEye, Crowdstrike, etc.
- Understand the top three Techniques, Tactics and Procedures (TTPs) for your industry (e.g., spear phishing, hacking, ransomware)
  - IDENTIFY CONTROL AREAS TARGETED MOST BY BAD ACTORS

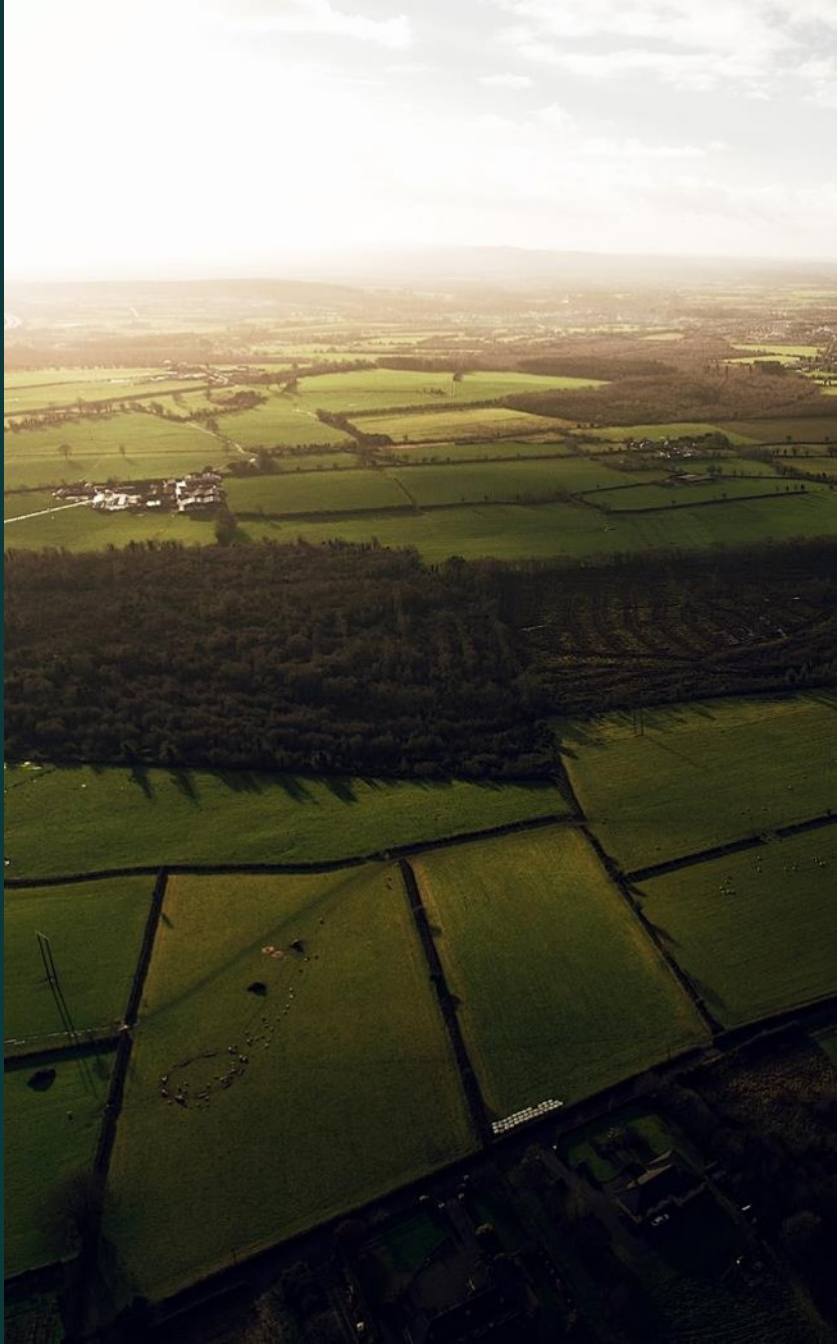
Recognize IT Security Perception of Audit

- Realize that not all IT Security teams understand audit value
  - KNOW HOW YOUR AUDIT TEAM IS PERCEIVED
- Are the Chief Auditor and Chief Security Officer cordial? Do they work collaboratively?
  - SET THE TONE AT THE TOP
- What is your personal reputation?
  - TECHNICAL, NON-TECHNICAL, NEW OR SEASONED
- Realize that time is precious, especially for IT Security teams
  - BE EFFICIENT

Set a Positive Tone

- Emphasize the shared common mission between Audit and Security
- Communicate the importance of audit efficiency
- Prepare and provide the list of reports or system reviews needed ahead of the audit
- Solicit IT Security feedback on high-risk target approach
- Reminder: Audit findings can help drive remediation projects and/or increase budgets

Effective Use of Audit Resources



A Risk-Based Approach to Allocate Resources

- Know what data types exist in your enterprise
  - PERSONALLY IDENTIFIABLE INFORMATION (PII)
  - PAYMENT CARD INDUSTRY DATA (PCI)
  - ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)
- Where is data located? What's the dark-web value? What are most common methods to compromise systems?
- Develop audit approach that emphasizes high-risk systems, threat actor methods, and corresponding controls
- Share audit approach with IT Security, get agreement and cooperation

Leverage Frameworks for Security and Compliance

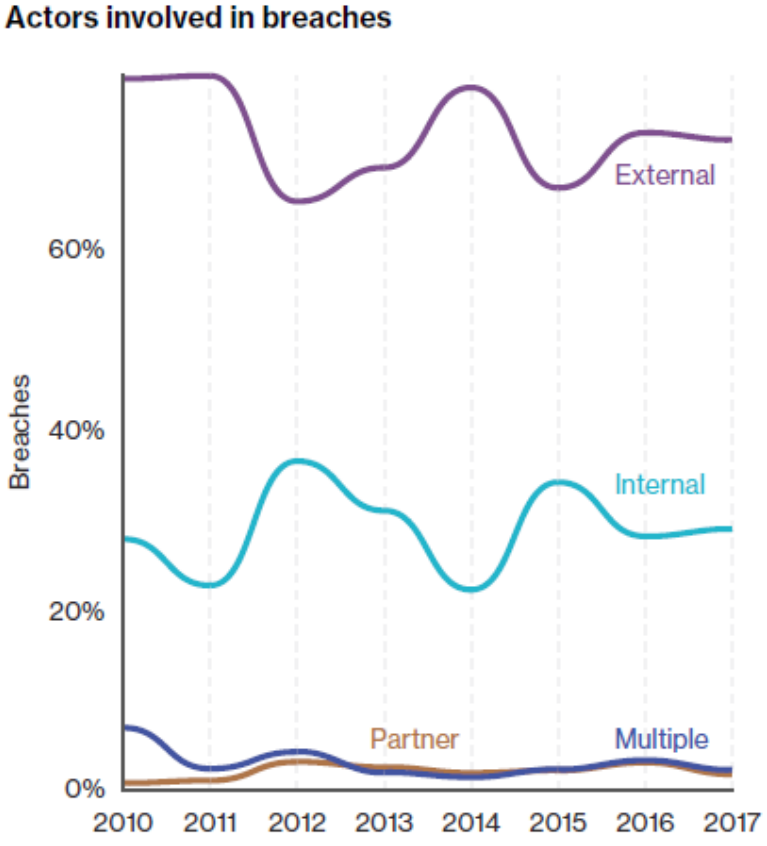
- Use established frameworks; consider using framework guidance across all areas of compliance
  - COSO FRAMEWORK (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION)
  - COBIT 5
- Know the security framework used by your information security team
  - NIST 800-53 OR 800-171, ISO 27001, HITRUST CSF, ETC., TO ASSESS SECURITY PROGRAM
- Review the appropriate framework, domains, and be conversant in it
- MITRE ATT&CK Matrix

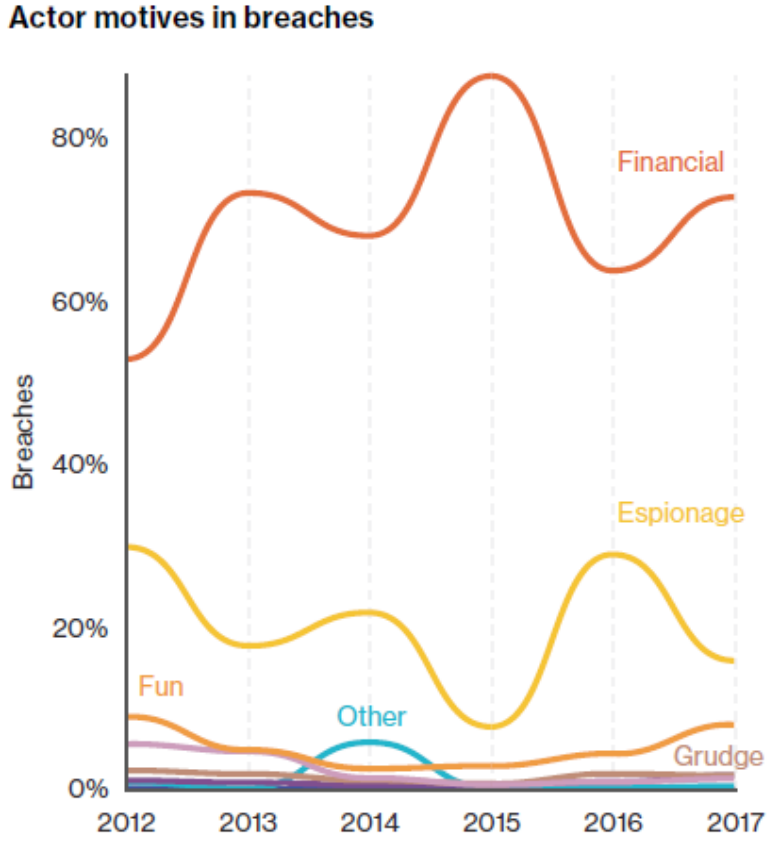
Key Techniques & Other Interesting Things

Tactics, Techniques and Procedures (TTPs)

- TTPs and “Tradecraft” are interchangeable
  - HOW THREAT ACTORS ORCHESTRATE AND MANAGE ATTACKS
- Know the Top 3 TTPs for your industry
- Healthcare
  - 43% EXTERNAL, 56% INTERNAL, 4% PARTNER
  - HUMAN ERROR, CRIMEWARE, PRIVILEGE MISUSE
- Retail
  - 93% EXTERNAL, 7% INTERNAL
  - DENIAL OF SERVICE, WEB APPLICATIONS, PAYMENT CARD SKIMMERS

Behind the Attack and a Look at Motivation





Audit Focused Examples

- Phishing
  - EMPLOYEE TRAINING PROGRAM
  - ANTI-PHISHING SOFTWARE
  - MALWARE PROTECTION (E.G., NEXT GENERATION ANTI VIRUS)
- Hacking
  - VULNERABILITY PROGRAM
  - PERIODIC THIRD-PARTY PENETRATION TESTING
  - WEB APPLICATION TESTING (DYNAMIC) AND/OR CODE REVIEW (STATIC)
- Credential Abuse
  - LEAST PRIVILEGE
  - DATABASE ANOMALY DETECTION

Key Takeaways

- IT Security is typically understaffed, underfunded, and over committed
- Audit and IT Security must be partners
- Study and learn IT security; become knowledgeable and respected
- Learn how threat actors compromise companies in your industry
- Utilize audit and IT security frameworks
- Design an audit that focuses on the vulnerabilities with the greatest impact

SURROUND YOURSELF

WITH THOSE ON THE SAME MISSION AS YOU

Questions?

Mark Edwards, CISM, CISSP

Senior Director of Cybersecurity

mark.edwards@mossadams.com

(858) 627-5530

Mark is an information security veteran with extensive experience in solving corporate cybersecurity problems using his deep knowledge and integrity. Mark has nearly 20 years' experience working as a deputy CISO, global cybersecurity and privacy consultant, and business developer covering a wide range of industry groups, regulations (GDPR, PCI, HIPAA/HITRUST CFS, etc.), and frameworks (NIST, ISO, CSF, COBIT, etc.).

Mark is passionate about helping clients avoid breaches that would need to be reported. His ability to protect commercial entities from cyber theft stems from a deep technical understanding of security technologies and solutions as well as a strong knowledge of global threats, particularly their tactics, techniques, procedures (TTPs) and compliance requirements. Prior to joining Moss Adams, Mark was a senior director with Endgame building relationships with new business in 13 western states with an advanced endpoint software agent. He was also the Deputy CISO at a $7B defense contractor.