Addressing penetration testing and vulnerabilities, and adding verification measures

July 25, 2017

Alan Calder
IT Governance Ltd
www.itgovernanceusa.com

PLEASE NOTE THAT ALL ATTENDEES ARE MUTED UPON JOINING
Introduction

- Alan Calder
- Founder of IT Governance Ltd
- Author of *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*
- Led the world’s first successful implementation of ISO 27001 (then BS 7799)
IT Governance – a leading global provider

• The single source for everything to do with cybersecurity, cyber risk management, and IT governance

• Our team of dedicated and knowledgeable trainers and consultants have helped over 400 organizations worldwide achieve ISO 27001 certification

• We are privileged to work with individuals and organizations from all business sectors and industries
Agenda

- Penetration testing
- Vulnerability assessments and monitoring
- Monitoring and training controls for employees
# NYDFS Cybersecurity Requirements compliance deadlines

<table>
<thead>
<tr>
<th>180 days</th>
<th>1 year</th>
<th>18 months</th>
<th>2 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 500.02 Cybersecurity Program</td>
<td>Section 500.04 (b) Chief Information Security Officer (CISO)</td>
<td>Section 500.06 Audit Trail</td>
<td>Section 500.11 Third Party Service Provider Security Policy</td>
</tr>
<tr>
<td>Section 500.03 Cybersecurity Policy</td>
<td>Section 500.05 Penetration Testing and Vulnerability Assessments</td>
<td>Section 500.08 Application Security</td>
<td></td>
</tr>
<tr>
<td>Section 500.07 Access Privileges</td>
<td>Section 500.09 Risk Assessment</td>
<td>Section 500.13 Limitations on Data Retention</td>
<td></td>
</tr>
<tr>
<td>Section 500.10 Cybersecurity Personnel and Intelligence</td>
<td>Section 500.12 Multi-Factor Authentication</td>
<td><strong>Section 500.14 (a) Training and Monitoring</strong></td>
<td></td>
</tr>
<tr>
<td>Section 500.16 Incident Response Plan</td>
<td><strong>Section 500.14 (b) Training and Monitoring</strong></td>
<td>Section 500.15 Encryption of Nonpublic Information</td>
<td></td>
</tr>
</tbody>
</table>
Financial sector vulnerabilities

7,111 financial services companies assessed by SecurityScorecard

1,356 out of these companies at least one unpatched vulnerability from the common vulnerabilities and exposures (CVE) database

72% of these companies were vulnerable to CVE 2014-3566 (POODLE)

38% were vulnerable to CVE 2016-0800 (DROWN)

23% were vulnerable to CVE 2015-0204 (FREAK)
Penetration testing and vulnerability assessments (Section 500.05)

• The cybersecurity program must include monitoring and testing in accordance with the risk assessment

• Monitoring and testing must consist of carrying out either:
  – Continuous monitoring
  – Or periodic Penetration testing and vulnerability assessments

• Any entity lacking effective continuous monitoring, or other systems to detect changes in information systems that may generate or point out vulnerabilities, must conduct both:
  – Annual Penetration Testing of the Covered Entity’s Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and
  – Bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity’s Information Systems based on the Risk Assessment.
Biggest problems in achieving NYDFS cybersecurity compliance

- A recent Ponemon Institute survey of NYDFS-covered companies reported that 69% of respondents said that the most difficult part of meeting the Cybersecurity Requirements was conducting annual penetration tests and implementing continuous monitoring.
Penetration testing

- A penetration test, or pen test, is an authorized attack on a computer system, carried out with the intention of finding security weaknesses, and gaining access to it, its functionality and data.

- Why should your organization conduct testing?
  - Regulatory compliance
  - Demonstrating due diligence
  - Providing risk-based assurance that controls are being implemented effectively
Why should you conduct a regular test?

• New vulnerabilities are identified and exploited by hackers every week, if not every day.

• In many cases, you won’t even know that your defenses have been successfully breached until it’s too late.

• The Federal Deposit Insurance Corporation (FDIC) was accused last year of covering up data breaches that occurred in 2010, 2011, and 2013. In each instance, the regulator’s computers were compromised by the Chinese government.
## Advantages of penetration testing

<table>
<thead>
<tr>
<th>EVALUATE</th>
<th>IDENTIFY</th>
<th>PRIORITIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurately evaluate your organization’s ability to protect its networks, applications, endpoints, and users from determined attackers.</td>
<td>Get detailed information on actual, exploitable security threats to identify which vulnerabilities are more critical, which are less significant and which are false positives.</td>
<td>More intelligently prioritize remediation, apply necessary security patches, and allocate security resources more effectively to ensure they are available when and where they are needed most.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COMMUNICATE</th>
<th>PROTECT</th>
<th>COMPLY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help IT security professionals communicate and prove the need for a security budget with business managers and non-tech folk.</td>
<td>Protect your company’s profits and reputation by avoiding the financial costs and negative publicity associated with a compromise of your systems.</td>
<td>Address the general auditing aspects of regulations and standards – such as the PCI DSS, ISO 27001, and the GDPR – and avoid significant fines for non-compliance.</td>
</tr>
</tbody>
</table>
Conducting a penetration test

- What needs to be tested:
  - Network layer
  - Application layer
  - User layer
  - Publicly accessible system
  - High-risk systems
  - High-value systems
  - Internal systems
  - Segmentation

Diagram:
- User attack surface
- Application attack surface
- Network attack surface
Internal or external testing

- **Internal simulation**
  - A malicious insider
  - The actions of a hacker who has gained access

- **External simulation**
  - An external threat
  - The actions of a hacker trying to gain access

- In 2016, the *New York Times* reported that the FBI had arrested a National Security Agency (NSA) contractor for stealing and sharing highly classified computer code developed by the NSA to hack into the networks of foreign governments.

- In 2015, an **FDIC employee** copied personally identifiable information of 40,000 individuals. Additionally, information on how 31,000 banks handle bankruptcy was copied to a thumb drive immediately before the employee left the FDIC. The drive was recovered months later.
Arranging a test

- Selecting a supplier
- Scoping the engagement
- Understanding the report
- Conducting remediation
Levels of attack

- **L1** - Mostly automated, high volume, always-on attack systems that search out and exploit known vulnerabilities.
- **L2** - Targeted attacks, aimed at breaking into high-value targets, which incorporate a significant human element.
- Penetration testing should be deployed to match the activity.

**L1**
- Monthly or quarterly
- Identifies known vulnerabilities from the CVE database and provides detailed remediation advice.
- As new vulnerabilities emerge every day, this sort of testing should be the standard practice.

**L2**
- Every 6 to 12 months
- More sophisticated
- Tests for linked vulnerabilities and weaknesses that a competent attacker could exploit.

Copyright IT Governance Ltd 2017 – v1.0
# Different test types

<table>
<thead>
<tr>
<th>Detail of test</th>
<th>Vulnerability Scan</th>
<th>L1 penetration test</th>
<th>L2 penetration test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternative names</td>
<td>Automated scan</td>
<td>Vulnerability</td>
<td>Full penetration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>assessment</td>
<td>testing</td>
</tr>
<tr>
<td>Pre-assessment client scoping and consultation</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Scope of assessment</td>
<td>Agreed with client</td>
<td>Agreed with client</td>
<td>Agreed with client</td>
</tr>
<tr>
<td>Can be conducted internally and externally</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Identification of potential vulnerabilities</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Identification of configuration vulnerabilities</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Identification of potential security loopholes</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Immediate notification of critical issues</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
</tbody>
</table>
## Different test types (continued)

<table>
<thead>
<tr>
<th>Detail of test</th>
<th>Vulnerability Scan</th>
<th>L1 penetration test</th>
<th>L2 penetration test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated scanning</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Manual scanning</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Manual testing</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Manual grading of vulnerabilities</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Exploitation of potential vulnerabilities to establish the impact of an attack</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
Credentials to look for in a penetration tester

• Can they provide evidence of a solid reputation, history and ethics (e.g. a full trading history, good feedback from both clients and suppliers, a reliable financial record, and a strong history of performance)?
• Do they take part in specialised industry events (such as those run by CREST or OWASP chapters)?
• Are they able to demonstrate exploits or vulnerabilities, you have found in other similar environments?
• Can they provide independent feedback on the quality of work performed and conduct of staff involved?
• Do they adhere to a formal code of conduct overseen by an independent industry body?
Scoping the penetration test: questions your provider should ask

- What are the business drivers behind needing/wanting to do a penetration test?
- What are the outputs you require from the testing? – Assurance/governance
- What threats are trying to protect against? – Internal/external
- What are the systems that need to be tested? – Critical/high profile/everything
- Are you testing infrastructure and applications or admin and monitoring systems?
Are third-party permissions required?

3rd Party Hosting Provider

Cloud Service Provider
Reporting – what is included and what can you expect to receive?

- Provide a detailed technical report on the vulnerabilities of the system.
- Explain the vulnerabilities in a way that is easily understood by senior management.
- Report the outcome of the test in business risk terms.
- Identify short-term (tactical) recommendations.
- Conclude with and define ‘root cause’/long-term (strategic) recommendations.
- Include a security improvement action plan.
- Provide assistance to the organization in implementing the security improvements.
Report findings

• Findings identified during the penetration test should be recorded in an agreed format and describe each finding in both:
  - Technical terms that can be acted upon
  - Non-technical, business terms, so that the justifications for the corrective actions are understood

• Reports should describe the vulnerabilities found, including:
  - Test narrative – describing the process that the tester used to achieve particular results
  - Test evidence – results of automated testing tools and screen shots of successful exploits
  - The associated technical risks and how to address them
ISO27001 and penetration testing

- **As part of the risk assessment process:** uncovering vulnerabilities in any Internet-facing IP addresses, web applications, or internal devices and applications, and linking them to identifiable threats

- **As part of the risk treatment plan:** ensuring that the controls that are implemented actually work as designed

- **As part of the continual improvement processes:** ensuring that controls continue to work as required and that new and emerging threats and vulnerabilities are identified and dealt with
Why ISO 27001?

- Internationally recognized standard
- Best-practice solution
- Substantial eco-system of implementers
- Leading companies have implemented
  - Wells Fargo
  - Citibank
  - The Federal Reserve Bank of New York
- Co-ordinates multiple legal and contractual compliance requirements
- Built around business-focused risk assessment
- Balances confidentiality, integrity, availability
- It’s possible to achieve certification in a timely and cost-effective manner
Annex A: 14 control categories

114 CONTROLS

5 Infosec policies

6 Organization of infosec

7 Human resources security

8 Asset management

9 Access control

10 Cryptography

11 Physical and environmental sec.

12 Operations security

13 Comms security

14 System acq., dev. & mtnce.

15 Supplier relationships

16 Infosec incident management

17 Infosec aspects of BC mgmt

18 Compliance
Employee training and monitoring controls (Section 500.14)

- As part of each cybersecurity program, the Covered Entity must:
  - implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users
  - provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment
ISO 27001 covers training and awareness

- A7.3 - Persons working within the ISMS must:
  - be aware of the information security policy
  - understand their contribution
  - understand the implications of non-conformance

- A7.2.2 - Information security awareness, education, and training should be proportionate to the role, including updates to policies and procedures

- Gaining management support and sponsorship for an awareness program is recognized as the most crucial aspect of the entire initiative
Staff training and awareness

- Password use and protection
- Virus protection
- Internet use and behavior that protects against malware
- Email use and behavior that protects against malware
- Confidential information protection
- Physical access
- Network access issues (such as modem use, home connection, log-in issues)
- Incident reporting
- Social engineering = exploiting human vulnerabilities
  - “Following instructions (or refusing to)”
  - Ignorance
  - Gullibility
  - Desire to be liked
  - Being helpful
Building a cybersecurity culture

• Establishing a threat-aware culture of institutional integrity and personal reliability. Provide regular staff awareness training, produce an Acceptable use policy governing IT resources, and create a safe environment in which security incidents can be reported without judgment

• Building a multi-disciplinary program to deter, prevent, detect, and respond to insider threats and to limit their impact

• Building and operating security controls, including access controls; data protection; configuration management; vulnerability and patch management; and internal network segmentation

• Monitoring and detecting insider behavior to prevent insider attacks by capturing observable indicators of potential activity before insiders act

• Developing and regularly testing an action plan for reacting to actual or suspected insider misbehaviour

• Evolving the approach as conditions change
Procedures, policies, and controls

- Implement a user account management system and privilege management process
- Don’t use network and system administrator user accounts for non-administrator activities
- Restrict special account privileges to a limited number of authorized individuals
- Don’t allow unauthorized user accounts access to applications, computers and networks
- Document user access permissions
- Implement a unique username and strong password policy
- Ensure user passwords are changed on a regular basis
Staff awareness program

- The best solution for all companies wishing to engage their staff with their cybersecurity strategy is a **staff awareness program**. Using training, tools, and thought-provoking activities, organizations can raise staff awareness of the daily cyber risks they face, and suggest actions and procedures to adopt to minimize such risks.

- A staff awareness program should be an ongoing process that begins with staff induction, and continues with periodic updates throughout the year and/or whenever any staff-related security incidents occur.
Benefits of staff awareness

• Helps companies identify potential security problems

• Helps staff understand the consequences of poor information security and cybersecurity

• Ensures procedures are followed consistently

• Ensures staff are fully aware of corporate compliance requirements for security regulations and frameworks such as the General Data Protection Regulation (GDPR), the PCI DSS, ISO 27001, HIPAA, and the GLBA
Valuable resources

• Free green papers:
  • Penetration testing and ISO 27001

  NYDFS Cybersecurity Requirements
  • Part 1 – The Regulation and the ISO 27001 standard
  • Part 2 – Mapped alignment with ISO 27001

• Data Sheet:
  • Penetration testing

• More information on ISO 27001 and the Regulation
  • www.itgovernanceusa.com/iso27001-nydfs-cybersecurity
Penetration testing (pen testing) packages
- www.itgovernanceusa.com/penetration-testing-packages

Staff security awareness and compliance training
- www.itgovernanceusa.com/itg-elearning
IT Governance offers two levels of penetration test to meet your budget and technical requirements

<table>
<thead>
<tr>
<th>Objective</th>
<th>Level 1 Penetration Test</th>
<th>Level 2 Penetration Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed-price package available</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Emulates a real-world attack</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scoping</td>
<td>High</td>
<td>Advanced</td>
</tr>
<tr>
<td>Skill level required</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Vulnerability scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can be performed on premise</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can be performed remotely</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Exploitation of vulnerabilities</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Detailed report</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual grading of responsibilities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Facilitates compliance with ISO 27001/the PCI DSS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

In most cases, we recommend a level 1 penetration test, which is a faster and more cost-effective solution at a fixed price, and will identify exploitable vulnerabilities and remediation solutions.

Level 2 Penetration Test

A more complete and painstaking test that aims to identify methods a criminal hacker could use to gain control of your system, enabling attacks deeper into your network.
eLearning courses

- IT Governance multi-user eLearning courses (whether generic or customized) can be hosted externally or internally.

- We offer the following hosting options:
  - Hosted in and delivered from our online learning environment. Staff simply log on to the selected training courses, and the nominated administrator can access online reports that show how many users have completed training, passed tests, etc.
  
  - Deployed in and delivered from your own network environment, on your own learning management system (LMS). All courses are SCORM 1.2- and AICC-compliant, and we also can provide you with an LMS for internal deployment if required.

  - You could also start with an external hosting environment and then, when you're ready, progress to an internal environment.
Customizable course content

- IT Governance courses can be rebranded to match your corporate identity so that your employees will enjoy an eLearning course experience that feels authentic, reinforces important brand messages, and enables you to make a bigger impact on your organization’s goals and objectives.

- We offer two different customization options for any course:
  - **Core customization** includes incorporating company policies and procedures, company contact information, corporate logos, and colour schemes according to a standard set of available customization options.
  - **Tailored customization** includes editing any additional element of the course and/or eLearning experience at an additional hourly charge, and is subject to a scoping call with your organization.
Choose from products that are tailored to NYDFS Cybersecurity Requirements and developed by expert practitioners

- ISO 27001 Certified ISMS online training
  - ISO 27001 Certified ISMS Foundation
  - ISO 27001 Certified ISMS Lead Implementer

- ISO 27001 Cybersecurity Documentation Toolkit
  - www.itgovernanceusa.com/shop/product/iso-27001-cybersecurity-documentation-toolkit

- vsRisk™ – risk assessment software
  - www.itgovernanceusa.com/shop/Product/vsrisk-standalone-basic

- ISO 27001 standard
  - ISO/IEC 27001 2013 (ISO 27001 Standard) ISMS Requirements
Questions and answers