NYS DFS Cybersecurity Requirements

Stephen Head
Senior Manager
Risk Advisory Services

December 5, 2017
About Me

**Stephen W. Head** – Mr. Head is a Senior Manager with Experis Finance, and has over thirty-five years of audit and technology experience spanning a variety of industries. He is a CPA, CGMA, CMA, CISA, CISM, CGEIT, CRISC, CISSP, CBCP, CFE, CHP, CHSS, CITP, CPCU, MCSE, and a MBA.

Stephen has published widely on the subject of auditing. He co-authored the AICPA’s *Statement on Auditing Standards No. 94* and is the author of the internationally recognized *Internal Auditing Manual* as well as *Practical IT Auditing*, both published by Thomson Reuters.

Stephen is a former ISACA Charlotte Chapter President and ISACA International Vice President. He served for two terms as the International Chair of the ISACA Standards Board, and was instrumental in the creation and rollout of the CISM certification. He also served on the AICPA National Accreditation Commission and was a member of the AICPA Information Technology Executive Committee.
Agenda

- What are the NYS DFS Cybersecurity Requirements?
- What is a Covered Entity?
- What Must be Completed and When is it Due?
- Tackling the Section 500.09 Risk Assessment
- Summary / Contact Information / Q&A
What are the New York State DFS Cybersecurity Requirements?
What are the New York State Cybersecurity Requirements?

Effective March 1, 2017, the Superintendent of Financial Services for the State of New York promulgated 23 NYCRR Part 500 (also known as Section 500), a regulation establishing cybersecurity requirements for financial services companies.

In addition to New York domiciled companies, this regulation also applies to numerous financial services companies that are licensed to do business in the State of New York and have at least $5,000,000 revenue in New York.
Why Did New York Implement Section 500?

A new ransomware attack is infecting airlines, banks, and utilities across Europe
Russell Brandam The Verge Jun 27, 2017

Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry
Thomas Fox-Brewster FORBES.COM Jun 27, 2017

Major Spammer Accidentally Leaks Data on a Billion People
Jonathan Vanian Fortune.com Mar 06, 2017

Major sites including New York Times and BBC hit by 'ransomware' malvertising
Theguardian | Alex Hern | 16 March 2016

Every single Yahoo account was hacked - 3 billion in all - Oct. 3, 2017
money.cnn.com/2017/10/03/technology/business/yahoo-3-accounts/index.html

Yahoo! Hack! How It Took Just One-Click to Execute Biggest Data Breach in History
Suval Khandelwal The HackerNews March 15, 2017

Change your passwords… again: Yet another Yahoo data breach affected 32 million accounts
Chris Smith BGR.com March 2, 2017

Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat
MANILA BY RAJU Gopalakrishnan AND MANUEL MOGATO Reuters May 19, 2016

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

U.S., Canada issue joint alert on 'ransomware' after hospital attacks
Reuters | By Jim Finkle | Mar 31, 2016

University pays $20,000 to ransomware hackers
BBC News June 8, 2016

Equifax: 15.2 Million UK Records Exposed - BankInfoSecurity
https://www.bankinfosecurity.com/equifax-152-million-uk-records-exposed-a-10372

Ransomware attack costs South Korean company $1M, largest ...
In their own words…

• The New York State Department of Financial Services ("DFS") has been closely monitoring the ever growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors.

• Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes.

• The financial services industry is a significant target of cybersecurity threats. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark.

• Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted.

• Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities.

Source: New York State DFS 23 NYCRR 500
Who is a Covered Entity?
Who is a Covered Entity?

Financial Services Companies licensed to do business in the State of New York, including those subject to:

- NYS Banking Law – Banks, Trusts, and Credit Unions
- NYS Insurance Law – Insurance Agents and Brokers
- NYS Financial Services Law – Mortgage, Investment and Holding Companies

Note that there are certain exemptions under Section 500.19. You should seek advice from your Legal Department for clarification.
Key Compliance Dates
Key Compliance Dates

- **March 1, 2017**: Effective Date of Cybersecurity Regulations (subject to transitional periods)
- **August 28, 2017**: 500.02 Cybersecurity Program, 500.03 Cybersecurity Policy
  - 500.04(a) CISO, 500.07 Access Privileges, 500.10 Cyber Personnel
  - 500.16 Incident Response Plan, 500.17(a) Event Notice to Superintendent
- **February 15, 2018**: 500.17(b) Annual Certification of Compliance
- **March 1, 2018**: 500.04(b) Annual Report by CISO
  - 500.05 Pen Test / VA, 500.09 Risk Assessment
  - 500.12 Multifactor Auth., 500.14(b) Awareness Training
- **September 1, 2018**: 500.06 Audit Trail, 500.08 Application Security
  - 500.13 Data Retention, 500.14(a) Monitoring
  - 500.15 Encryption of Nonpublic Information
- **March 1, 2019**: 500.11 Third Party Service Providers
August 28, 2017
Due Date
Section 500.02 – Cybersecurity Program

• (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity’s Information Systems.

• (b) The cybersecurity program shall be based on the Covered Entity’s Risk Assessment and designed to perform the following core cybersecurity functions:
  – (1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity’s Information Systems;
  – (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity’s Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;
Section 500.02 – Cybersecurity Program

– (3) detect Cybersecurity Events;
– (4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;
– (5) recover from Cybersecurity Events and restore normal operations and services; and
– (6) fulfill applicable regulatory reporting obligations.

• (c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

• (d) All documentation and information relevant to the Covered Entity’s cybersecurity program shall be made available to the superintendent upon request.
Section 500.03 – Cybersecurity Policy

• Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity’s board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity’s policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity’s Risk Assessment and address the following areas to the extent applicable to the Covered Entity’s operations:
  – (a) information security;
  – (b) data governance and classification;
  – (c) asset inventory and device management;
  – (d) access controls and identity management;
Section 500.03 – Cybersecurity Policy

- (e) business continuity and disaster recovery planning and resources;
- (f) systems operations and availability concerns;
- (g) systems and network security;
- (h) systems and network monitoring;
- (i) systems and application development and quality assurance;
- (j) physical security and environmental controls;
- (k) customer data privacy;
- (l) vendor and Third Party Service Provider management;
- (m) risk assessment; and
- (n) incident response.
Section 500.04(a) – CISO

• (a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity’s cybersecurity program and enforcing its cybersecurity policy. The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:
  – (1) retain responsibility for compliance with this Part;
  – (2) designate a senior member of the Covered Entity’s personnel responsible for direction and oversight of the Third Party Service Provider; and
  – (3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.
Section 500.07 – Access Privileges

• As part of its cybersecurity program, based on the Covered Entity’s Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.
Section 500.10 – Cyber Personnel and Intelligence

• (a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:
  – (1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity’s cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;
  – (2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and
  – (3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

• (b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.
Section 500.16 – Incident Response Plan

• (a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity’s Information Systems or the continuing functionality of any aspect of the Covered Entity’s business or operations.

• (b) Such incident response plan shall address the following areas:
  – (1) the internal processes for responding to a Cybersecurity Event;
  – (2) the goals of the incident response plan;
  – (3) the definition of clear roles, responsibilities and levels of decision-making authority;
  – (4) external and internal communications and information sharing;
Section 500.16 – Incident Response Plan

- (5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- (6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and
- (7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.
Section 500.17(a) – Event Notice to Superintendent

• (a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:
  – (1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
  – (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.
February 15, 2018
Due Date
Section 500.17(b) – Annual Certification

- (b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.
March 1, 2018
Due Date
Section 500.04(b) – Annual Report by CISO

• (b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity’s board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity’s cybersecurity program. The CISO shall report on the Covered Entity’s cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:
  – (1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity’s Information Systems;
  – (2) the Covered Entity’s cybersecurity policies and procedures;
  – (3) material cybersecurity risks to the Covered Entity;
Section 500.04(b) – Annual Report by CISO

- (4) overall effectiveness of the Covered Entity’s cybersecurity program; and
- (5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.
Section 500.05 – Pen Test / Vulnerability Assessment

• The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity’s Risk Assessment, designed to assess the effectiveness of the Covered Entity’s cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

• (a) 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
Section 500.05 – Pen Test / Vulnerability Assessment

• (b) 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.
Section 500.09 – Risk Assessment

• (a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity’s Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity’s Information Systems, Nonpublic Information or business operations.

• The Covered Entity’s Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity’s business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.
Section 500.09 – Risk Assessment

• (b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:
  – (1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;
  – (2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity’s Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and
  – (3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.
Section 500.12 – Multifactor Authentication

• (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

• (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity’s internal networks from an external network, unless the Covered Entity’s CISO has approved in writing the use of reasonably equivalent or more secure access controls.
Section 500.14(b) – Awareness Training

As part of its cybersecurity program, each Covered Entity shall:

• (b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.
September 1, 2018
Due Date
Section 500.06 – Audit Trail

- (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:
  - (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and
  - (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

- (b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.
Section 500.08 – Application Security

• (a) Each Covered Entity’s cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity’s technology environment.

• (b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.
Section 500.13 – Limitations on Data Retention

- As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.
Section 500.01 – Definitions

• (g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

  – (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers’ license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual’s financial account, or (v) biometric records;

  – (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.
Section 500.14(a) – Monitoring

As part of its cybersecurity program, each Covered Entity shall:

• (a) 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;
Section 500.15 – Encryption of Nonpublic Information

• (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.
  – (1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity’s CISO.
  – (2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity’s CISO.
Section 500.15 – Encryption of Nonpublic Information

• (b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.
Section 500.11 – Third Party Service Provider

- (a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:
  - (1) the identification and risk assessment of Third Party Service Providers;
  - (2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;
  - (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and
Section 500.11 – Third Party Service Provider

- (4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

- (1) the Third Party Service Provider’s policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

- (2) the Third Party Service Provider’s policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;
Section 500.11 – Third Party Service Provider

– (3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity’s Information Systems or the Covered Entity’s Nonpublic Information being held by the Third Party Service Provider; and

– (4) representations and warranties addressing the Third Party Service Provider’s cybersecurity policies and procedures that relate to the security of the Covered Entity’s Information Systems or Nonpublic Information.

• (c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.
500.09 Risk Assessment – One Suggested Approach
What is NIST?

About NIST

• National Institute of Standards and Technology
• Part of the U.S. Department of Commerce
• NIST’s mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
• 3,000 employees
• 2,700 guest researchers
• Two main locations: Gaithersburg, MD and Boulder, CO

NIST Priority Research Areas

- Advanced Manufacturing
- IT and Cybersecurity
- Healthcare
- Forensic Science
- Disaster Resilience
- Cyber-physical Systems
- Advanced Communications
NIST Cybersecurity Framework

Each NIST function has multiple categories subdividing the cybersecurity requirements into more detailed groups of activities. These categories are further divided into over 100 subcategories.

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
</table>
| • Asset Management  
• Business Environment  
• Governance  
• Risk Assessment  
• Risk Management Strategy | • Access Control  
• Awareness & Training  
• Data Security  
• Information Protection & Procedures  
• Maintenance  
• Protective Technology | • Anomalies & Events  
• Security Continuous Monitoring  
• Detection Processes | • Response Planning  
• Communications  
• Analysis  
• Mitigation  
• Improvements | • Recovery Planning  
• Improvements  
• Communications |

What assets need protection?  
What safeguards are available?  
What techniques can identify incidents?  
What techniques can contain impacts of incidents?  
What techniques can restore capabilities?
## Conducting a Cybersecurity Risk Assessment

<table>
<thead>
<tr>
<th>Function (Framework Core)</th>
<th>Category</th>
<th>Subcategory</th>
<th>Current Tier</th>
<th>Target Tier</th>
<th>Inherent Risk Probability (1 - 5)</th>
<th>Inherent Risk Impact (1 - 5)</th>
<th>Inherent Risk Score (Probability x Impact)</th>
<th>Residual Risk Score (Current State)</th>
<th>Residual Risk Score (Future Target State)</th>
<th>Recommended Activity (Target State)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTECT (PR)</td>
<td>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordinafinancial services industry among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</td>
<td>PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.</td>
<td>Tier 1: Partial</td>
<td>Tier 3: Repeatable</td>
<td>3</td>
<td>4</td>
<td>12</td>
<td>12</td>
<td>4</td>
<td>* Design and implement a continuous monitoring process. Ensure the monitoring objectives are defined. * Document the process in policies and procedures.</td>
</tr>
<tr>
<td>PROTECT (PR)</td>
<td>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordinafinancial services industry among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</td>
<td>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.</td>
<td>Tier 2: Risk Informed</td>
<td>Tier 3: Repeatable</td>
<td>4</td>
<td>5</td>
<td>20</td>
<td>12</td>
<td>7</td>
<td>* Enhance the IR Plan to be more complete and detailed. Ensure that cybersecurity is included. * Complete the effort underway to create a business continuity and disaster recovery plan for critical applications for the DI.</td>
</tr>
</tbody>
</table>
Summary
Essential Governance and Control Practices

- Risk assessment to evaluate IT security posture
- Relevant security policies
- Appointment of CISO with enterprise-wide responsibility
- Annual report by CISO to senior management
- Expert IT security personnel
- Training and awareness activities
- Incident response management plan
- Metrics to evaluate the efficiency and effectiveness of IT security operations
- Monitoring of business partners, vendors, third-parties
- Multifactor Authentication and Encryption
- Adherence to standardized security requirements (NIST, etc.)
Q&A / Contact Information
Contact Information

Stephen Head, CISSP, CISM, CISA
Senior Manager, Risk Advisory Services
Mobile: 704.953.6688
Email: stephen.head@experis.com

Thank You for Attending!