Data Privacy and Cybersecurity for Higher Education Institutions

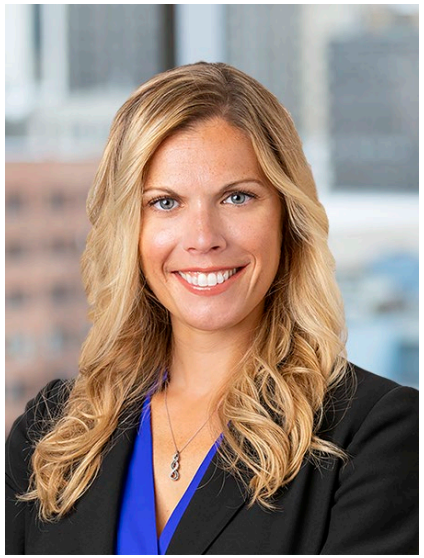
Webinar Series – Part Four

Higher Education Cybersecurity & Data Breach Response

April 13, 2023

BOND SCHOENECK & KING ATTORNEYS

Introductions



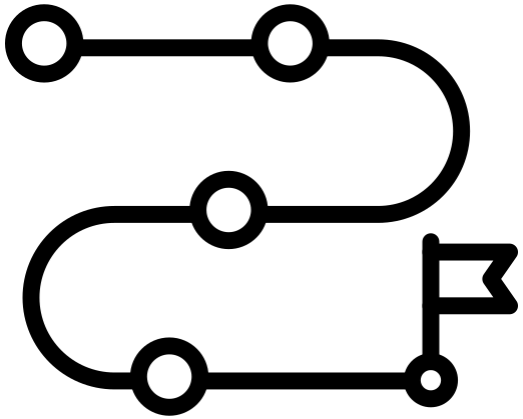
Jessica L. Copeland
Member – Buffalo, NY
Chair – Cybersecurity and Data Privacy Practice
jcopeland@bsk.com | (716) 416-7034
bsk.com/people/jessica-l-copeland

Seth F. Gilbertson
Senior Counsel – Buffalo, NY
Labor and Employment Practice Group
sgilbertson@bsk.com | (716) 416-7130
bsk.com/people/seth-f-gilbertson

BOND SCHOENECK & KING ATTORNEYS

Overview

- Key definitions
- Common types of data breaches
- Data breaches in higher education
- Recent data breaches
- Breach response strategy
- Implementing policies and procedures
- Information management best practices



Key Definitions

- **Personal Information** - any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify a person.

- **Private Information** – any information in combination with any one or the following: SSN; DL/ID number; financial account number; credit or debit card number; biometric information; or username or e-mail address in combination with a password or security question and answer.

- **Data Breach** - unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business.

Common Data Breaches

- **Inadvertent Disclosure/User Error**
  - Most common data incident
  - Not caused by a bad actor

- **Malware** – intrusive software designed to steal or damage data and computer system (Spyware, Adware, Worms, Trojans, Botnets)

- **Ransomware** – one of the most popular subsets of malware designed to encrypt or render files unusable (Lock Bit, Phobos, Royal, etc.)

- **Phishing** – a form of social engineering designed to deceive recipients into revealing confidential information

Data Breach in Higher Ed – ED Guidance

Data breaches can take many forms including:

- hackers gaining access to data through a malicious attack;
- lost, stolen, or temporary misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);
- employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.); and
- policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable).

Data Breaches in Higher Ed

- Colleges and Universities are frequent targets for cyber attacks
  - Retain large amounts of student records
  - Records often contain high value information such as SSNs, addresses, ID numbers, and financial information.

- As of 2022, ransomware attacks targeting higher education average about $2.7 million in recovery costs.

- Ransomware response costs about $1.8 million on average.

- The higher average cost for colleges and universities can be attributed to:
  - Siloed, department specific data storage practices, and
  - Outdated and infrequent backup and recovery systems.

Source - Emma Whitford, *Cyberattacks Pose 'Existential Risk' To Colleges—And Sealed One Small College's Fate*, Forbes (April 19, 2022)

Recent Data Breaches in Higher Education

- **April 2023 -** the University of Hawaii Maui College reported unauthorized access to approximately 10,500 student records containing confidential information.

- **March 2023** - Our Lady of the Lake University posted a notice of data breach on its website after the institution learned that an unauthorized party was able to access and remove files containing names, SSN, DL/ID numbers, passport numbers, government identification number, DoB, and bank account information.

- **February 2023** – Stanford University sent data breach notification letters to 897 individuals who submitted personal and health information as part of the graduate application. Stanford reported that it found evidence that the files were downloaded off their system.

- **February 2023** - Mount Saint Mary College reported the unauthorized access of confidential records belonging to 17,924 students and employees.

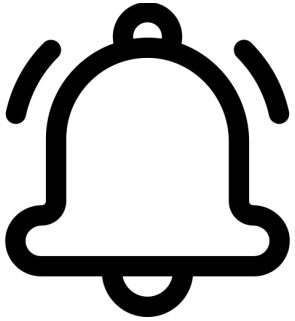
Responding to a Data Breach: Identify the Threat

- Detect the incident
- Contact breach response team
- Response team meets to determine whether an incident is ongoing based on available evidence and set criteria in the incident response plan
- Direct IT to isolate the threat:
  - Business email compromise – disable email account
  - Ransomware attack – quarantine impacted server(s) and take offline

Responding to a Data Breach: A Team Effort

- Contact insurance carriers – cyber liability insurance typically covers:
  - Legal and forensic investigation fees associated with a data incident
  - Voluntary and mandated notifications to impacted individuals and regulators
  - Business interruption expenses attributable to a data incident
- Engage forensic team – an investigation will identify and preserve evidence pertaining to an intrusion.
- Engage cyber counsel – relying on the forensic team's findings, counsel will determine whether the incident rises to the level where reporting is required.
- Engage local and federal law enforcement if necessary.

Notification Procedures and Obligations (NY)



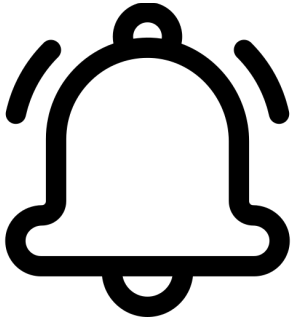
- If a data incident triggers reporting requirements, notification may be required to impacted individuals, regulators, and/or credit reporting agencies.

- **Individual Notice** - include contact information, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization.

- **Regulator Notice** – if any notifications are made to NY residents, notification must also be provided to the state AG, department of state, division of state police, and U.S Department of Education.

- **CRAs –** notice only required if more than 5,000 NY residents were notified.

Notification: Governing Authority



- **Statutory Authority** – N.Y. Gen. Bus. Law § 899-aa (McKinney)
  - Requirement to disclose any breach to any resident of NYS whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization, accessed or acquired by a person without valid authorization
  - Notice is not required if the incident was inadvertent by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm.

- **Contractual Authority** – FSA's Title IV Student Aid Internet Gateway (SAIG) Agreement
  - Postsecondary intuitions (PSIs) that distribute Title IV funds enter into agreements with FSA via a Program Participation Agreement (PPA) and a SAIG Agreement. Those agreements include stipulations about safeguarding data.
  - The SAIG Agreement requires that as a condition of continued participation in the federal student aid programs, PSIs report actual data breaches, as well as suspected data breaches. Title IV PSIs must report on the day that a data breach is detected or even suspected.

International Law

When collecting information from prospective students or alumni residing outside the U.S., determine whether any additional privacy authorities govern this data.

- **European Economic area and United Kingdom - GDPR**
  - The EEA and UK versions of the General Data Protection Regulation are compressive consumer privacy laws
  - Controllers must notify their supervisory authorities within 72 hours of a breach
  - Individuals impacted by a breach must be notified without undue delay

- **China - PIPL**
  - The Personal Information Protection Law is China's compressive consumer privacy authority
  - Where personal information has been disclosed, altered, or lost, or is likely to, the personal information handler must immediately take remedial measures and notify the responsible State Authority and affected individuals
  - Lawful data transfer mechanisms currently in flux

Implementing or Revising Policies & Procedures: Policy

- Create a data breach response policy, approved by leadership. The purpose of the policy is to establish goals and vision for the breach response process.

- Policy should have a clearly defined scope (to whom it applies and under what circumstances), and it should include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms.

- The policy should be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Implementing or Revising Policies & Procedures: Plan

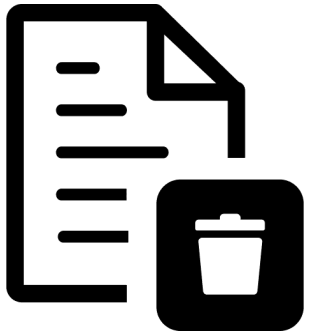
- A data breach response plan is a high-level strategy for implementing the data breach policy. Individual elements of the plan should cover all phases of the incident response, from reporting the breach and the initial response activities to strategies for notification of affected parties, to breach response review and remediation process.

- The plan should identify the necessary organizational resources and required management support, such as senior management approval. It is important that the plan is highly tailored to mission, goals and risks.

Implementing or Revising Policies & Procedures: Procedures

- Procedures are derived from the breach response plan and codify specific tasks, actions, and activities that are a part of the data breach response effort.
- Procedures are designed to standardize behavior to ensure that response activities are handled in an efficient, documented, and repeatable way, while minimizing the introduction of errors.
- Breach response procedures should be periodically reviewed and tested in conjunction with other business continuity and disaster recovery procedures to test their effectiveness and identify areas for improvement.

Information Management Best Practices: Record Retention



- **Schedules** – create an internal policy that establishes when certain types of data must be deleted

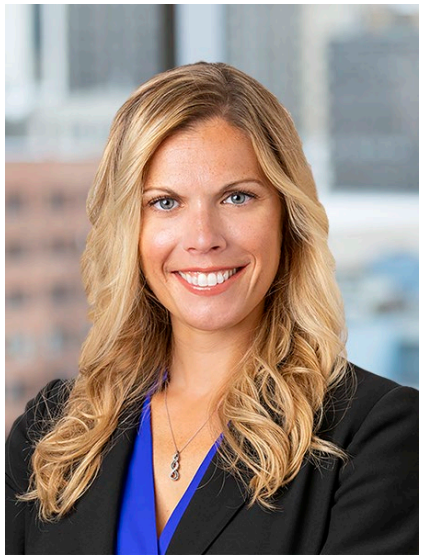
- **Custodians** – responsibility for specific systems and records should be clearly stated in the retention schedule and any vendor/sub processor agreements

- **Enforcement** – all record retention policies should be tested regularly via risk assessments and tabletop exercises. Employee penalties for failure to comply may range from additional training to termination.

Information Management Best Practices: Security Protocol

- **Administrative Safeguards**
  - Written Information Security Plan
  - Incident Response Plan
  - Business Continuity Plan
  - Workforce training
- **Physical Safeguards**
  - Facility security plan
  - Physical media destruction protocol
  - Building access controls and identity verification
- **Technical Safeguards**
  - Access controls
  - Encryption
  - Backup and integrity controls
  - Unique user identification
  - Multifactor authentication
  - Automatic logoff

Questions?



Jessica L. Copeland
Member – Buffalo, NY
Chair – Cybersecurity and Data Privacy Practice
jcopeland@bsk.com | (716) 416-7034
bsk.com/people/jessica-l-copeland

Seth F. Gilbertson
Senior Counsel – Buffalo, NY
Labor and Employment Practice Group
sgilbertson@bsk.com | (716) 416-7130
bsk.com/people/seth-f-gilbertson

BOND SCHOENECK & KING ATTORNEYS

Thank You

The information in this presentation is intended as general background information.
It is not to be considered as legal advice.
Laws can change often, and information may become outdated.