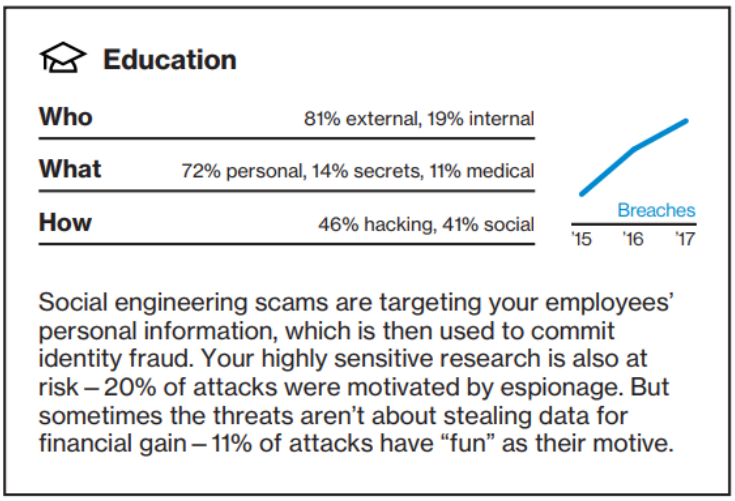
Protecting Student Data is Your Obligation –

What is your school's GPA?

Every day, we are confronted with headlines of a data breach in some sector of industry that demonstrates how prevalent breaches have become and the costs to remediate these breaches can be truly staggering. Not only is your college or university providing an important service in educating others but it must also recognize and accept its role as a guardian of sensitive data. Some of this data may be the most sensitive that a student will ever share with any organization, such as medical and mental health information as well as financial records. And since students often have little in the way of credit records, cyberthieves are especially attracted to student identity data.[1]

What complicates the safeguarding process are the many types of data in today's colleges and universities, such as student education records, health data, financial aid and research, and each type has its own regulatory oversight. Abiding by all of these can be an intimating process especially since there is increased concern by federal agencies and state governments over data breaches. However, it can become less intimidating if your school looks at this in a wholistic approach. This can help get your arms around your school's current capabilities and protections. Surprisingly, many of the regulations appear very repetitive since they talk about similar safeguards that need to be in place. This is because the regulations approach security standards in what are considered best business practices regardless of the industry. A great example is that most or all regulations call for "appropriate administrative, technical and physical safeguards" to ensure the security and confidentiality of data, to protect against reasonably anticipated threats and to guard against unauthorized access to these data sets.



According to a report by Verizon[2], "social attacks" figure prominently in academia, probably because of the "open" culture of schools and universities. It is far more common to find names, job roles, and contact information of school workforce (staff and faculty) than is typical in other industries. This clearly aids the bad actors in who to target.

Also, according to the Verizon report, "denial-of-service" attacks remain extremely common in Education, and cyber-espionage is still a significant pattern" in the breaches being reported. While cyber-espionage is responsible for less than 8% of breaches across all industries, it is responsible for 25% of the breaches in the Education sector. So, according to the Verizon report, "… whether they are interested in highly sensitive research, the technical specs for collaborative projects with major industry or simply the details of safe-space allocation, it is clear that the bad guys still want to know what our educational entities are up to."

---

1 "Case Study: Education" by KnowBe4, Inc, available at: https://www.knowbe4.com/hubfs/Education.pdf

2 "2018 Data Breach Investigations Report" by Verizon in collaboration with numerous agencies, subtitled as "Tales of dirty deeds and unscrupulous activities."

The Internet of Things (IoT)will grow as a vector for hackers— Gitanjali, a cybersecurity vendor, predicts that the number of IoT attacks to increase to 300,000 in 2019, and to account for more than 30 percent of all cyberattacks. By contrast, the firm estimates there were 50,000 such attacks in 2017. "With more unprotected IoT devices connecting to IT networks, we will potentially see more pronounced and larger scale cyberattacks driven by IoT botnets," the firm predicts.

According to reports by Gartner[3]:

- Consumers are increasingly moving their business to where organizations their personal information is best protected and cared for.
- By 2020, national authorities in the U.S. and U.K. will mandate capture of information related to cybersecurity breaches.
- By 2021, at least one company will publicly acknowledge a $1 billion revenue impact from a business outage resulting from a malware/ransomware attack.
- By 2022, cybersecurity ratings will become as important as credit ratings when assessing the risk of business relationships.

Something important to understand is that while you can have a strong information security program without a strong privacy program, the reverse is not true. As former DHS Director, Michael Chertoff once said, "You cannot have privacy without security."

This white paper is designed as a self-assessment providing a few of the many questions you should be asking to get a sense of your school's "GPA," or ***General Privacy Assessment***.

TOPIC: OVERALL READINESS

Many steps need to be taken to ensure your school is protecting the privacy of the data it has collected. Various disciplines are required to implement technical safeguards, to write appropriate policies and training plans, to assess current protocols, to perform risk analyses of systems, and so on.

Your college or university may be among the few to have the internal resources in place to handle all of these tasks but the opposite is most likely true. There needs to be a fair and objective assessment about those resources. Sometimes, an outside review by experienced professionals can make sense to ensure the right pieces are in place.

Definitions:

- *Administrative safeguards* – Documented policies, procedures and plans that address privacy and information security requirements
- *Technical safeguards* – Technical components of systems that provide a secure infrastructure for creating, storing, using, and transmitting information
- *Physical safeguards* – Operational practices that help ensure protected use and sharing of information
- *Denial-of-service (DoS) attacks* – Attacks that typically flood servers, systems or networks with traffic in order to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them.

[3] "Predicts 2018: Security and Risk Management Programs", Gartner - July 2018 and "Build for Privacy," Gartner - June 2018

Q: Readiness – Do we have the right people, protocols and budget needed to protect our data?

- ☐ Do we have a Privacy Official who is trained in FERPA[4], HIPAA[5], GLBA[6], GDPR[7] and relevant state laws, such as the California Consumer Privacy Act?
  - o If so, does this person have the budget and tools necessary for tracking and reporting breaches?
- ☐ Do we have a Chief Information Security Official with high-level authority?
  - o If so, does this person have sufficient staffing, budget, and tools to ensure a secure infrastructure?
- ☐ Does the university have a cybersecurity plan in place that covers all aspects of cybersecurity, not just those associated with personal information?
- ☐ Does the university's current insurance cover cybersecurity incidents?
- ☐ Do we have a campus-wide Information Management Committee to address all of the regulations we face?
  - o If so, how is the school's leadership kept informed of its activities and findings?
- ☐ Have we conducted periodic risk assessments of our systems, and practices?
- ☐ Do we have an Incident Response Plan in place?
  - o If so, has it been updated, audited and tested in the last 12 months?
  - o Are there developed, easy-to-follow playbooks and flowcharts that have been rehearsed in a tabletop exercise?
  - o Have representatives from non-IT departments also participated in the tabletop exercise? (Examples include human resources, marketing, legal, privacy, compliance, and even the finance director)
- ☐ Do we have an Incident Response Team identified and trained?
- ☐ When and how will our leadership be notified about cybersecurity incidents or breaches, consistent with escalation steps in the Incident Response Plan?
- ☐ Do our mission-critical systems containing sensitive information have log files of all transactions performed?
  - o If so, are those logs reviewed for inappropriate activities?
  - o Is suspicious activity investigated, reported and tracked?
  - o Are all users aware their activities are logged by the system?
  - o Are all users aware of the consequences for misuse of system access privileges?
- ☐ Are there progressive discipline policies in place to address privacy violations in a clear and decisive manner?
- ☐ Is the school investing heavily in online educational offerings to our students?
  - o If so, do we have safeguards in place to protect against DoS attacks?
  - o Do we have a mitigation plan in place if a DoS attack occurs?
- ☐ Are we capable of answering these questions (for all systems) fairly and objectively with internal staff?

[4] FERPA = Family Educational Rights and Privacy Act of 1974

[5] HIPAA = Health Insurance Portability and Accountability Act of 1996

[6] GLBA = Gramm-Leach-Bliley Act of 1999

[7] GDPR = General Data Protection Regulation 2016/679 (European Union (EU) regulation on data protection and privacy of EU citizens)

TOPIC: SOCIAL ENGINEERING

Definitions:

- *Social Engineering* – An attack vector that relies on people with some level of system access to give up their login user ID and password
- *Phishing email* – A type of Social Engineering done through email sent to as many people as possible to persuade individuals to provide sensitive information and/or take action through seemingly trustworthy communications.[8] For example, it may appear to be from PayPal and ask the recipient to verify their account details. These may be sent to many people in the university because the attacker assumes there will be a low response rate.
- *Spear phishing* – An attack in which a perpetrator, disguised as a trusted individual, attempts to trick a target into clicking a link in a spoofed email, text message or instant message. As a result, the target unwittingly reveals sensitive information or even installs malicious programs (malware) on their network. These attacks are targeted at a category of people with lower profiles in the organization.
- *Whaling* – A phishing email that is targeted exclusively at people in upper levels with access to highly valuable information, including research, trade secrets, etc.
- *Ransomware* – A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid

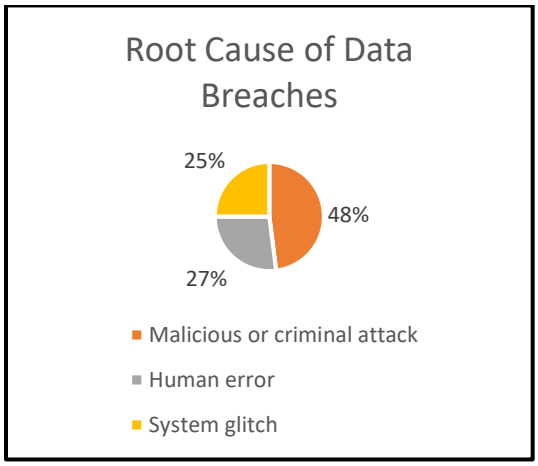
"Social engineering" is one of the most prevalent ways for systems to be illegally accessed. This is most commonly done through email, i.e. "phishing email" where the attackers are usually trying to pass themselves off as someone the recipient knows, like their supervisor, or someone the recipient should trust, like the school's IT Help Desk. Invariably, the email is asking the person to click on a link and login to a website thinking they are doing something that is okay or even GOOD to do, like reclaiming their email inbox. But by logging in, they are actually giving up their login user ID and password which will be used to gain access to their system accounts to see what information is available. The attackers may then pass themselves off as this victim in other phishing emails to gain more access or data or money from other people or systems.

"Phishing campaigns" are where the school's IT department sends phishing emails as a test to see who will click on links and give up their login credentials. It's sad to say but many times, the culprits that let the bad actors into systems to steal student data are the students themselves. Our experience with phishing campaigns in colleges and universities is that students will often click on almost anything if it seems like a good idea or if they think they will somehow benefit from it. That is why your students must be included as part of the overall training focus.

"Ransomware" is often delivered as an attachment to an innocent looking email that a user will likely open causing the malware program to encrypt key files and even back-up drives preventing a restoration of systems. Ransomware can also occur when a user unknowingly visits an infected website causing the malware to download and install without the user's knowledge. Newer methods of ransomware infection are spreading through social media.

[8] *See* Mark Smith, *Social Engineers Reveal Why the Biggest Threat to Your Business Could Be You*, *available at:* https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat- business .

According to an IBM/Ponemon Institute report[9], the second leading root cause of data breaches is the human factor.



Q: Social Engineering – How vulnerable are we to this kind of attack?

- ☐ Do we perform phishing campaigns on our workforce?
  - o If so, then:
    - ☐ Do we notify individuals when they "failed" the test?
    - ☐ Do we follow-up with the respective manager to let them know who needs additional training?
- ☐ Do we perform phishing campaigns on our student population?
- ☐ Do we allow our workforce to use campus workstations for their private email and personal social media?
- ☐ Do we allow our workforce to access secure wireless networks with their personal mobile devices?
- ☐ Do we have a strong web-filtering program to block known or suspected dangerous websites?

TOPIC: TRAINING

Regardless of the technological tools we can put in place, the weakest link in the chain to protect sensitive information is the human element. Those with email accounts (workforce and students) are the front line of defense. Technical security controls can be rendered useless with one careless mouse click by a user. According to Cofense[10], even though phishing attacks increased by 65% in 2017, extensive training efforts in some companies have dropped the success rate for attacks to as low as 5%. This is significant since phishing is the most common way to deliver ransomware.

Another important consideration in the college/university environment is the impact of students can and do have on protecting systems. While they may have amazing skills with today's technology, it is not axiomatic that they are well-versed in how to protect their data or system access accounts. According to Eyong B. Kim[11], the key to ensuring that students participate in the necessary training, schools should consider several approaches, such as:

- During new student orientation
- When they first login to the school's learning management system at the beginning of each semester
- At the time they register for classes

---

9 "2018 Cost of a Data Breach Study: Global Overview," benchmark research sponsored by IBM Security and independently conducted by Ponemon Institute, LLC.

10 "2017 Enterprise Phishing Resiliency and Defense Report," by Cofense, Inc., available at: https://cofense.com/phishing-resiliency-%20report-2017/

11 Kim, Eyong B., "Recommendations for Information Security Awareness Training for College Students," Information Management & Computer Security, Volume 22, Issue 1, 2014, available at: www.emeraldinsight.com/0968-5227.htm

Definition:

- *Training* – Provides the skills to do something rather than just know about something. As educators, your faculty members know all the theories of providing education to students. But here we're talking about ***training***. For example, in Physics class students may learn the theory of how to split an atom (education) but they do not receive *training* to ***actually split an atom***.

Q: Training… Are we doing a good job with training our staff, faculty and students about privacy and security?

- ☐ Do we have a thorough, documented plan for training of the workforce in privacy and information security to the depth needed based upon their role ("one size may not fit all")?
- ☐ Do we mandate privacy and information security training for ALL new hires, *including faculty and student employees*?
- ☐ Do we track those people that have and have not taken this training?
- ☐ Do we include all students in some degree of information security training?
- ☐ Do we have an "acceptable use of technology" policy?
    - If yes, do we require all to read it and then sign an acknowledgement of our expectations and their responsibilities?
- ☐ Do we have a "Confidentiality Agreement" for people to sign acknowledging their role in protecting sensitive information?
- ☐ Are we providing periodic reminders of what good privacy and information security practices look like?
- ☐ Do we require annual re-training?
- ☐ Does training include the knowledge to recognize potential issues as they happen?
- ☐ Do we publicize who to contact if a problem arises with suspicious emails or unusual requests from leadership?

TOPIC: STUDENT EMPLOYEES

Colleges and universities probably could not survive without student workers and certainly, these students appreciate the opportunity to learn new skills while earning income to help defray the cost of their education. Nonetheless, it is incumbent upon the school to ensure this population follows the same acceptable use policy and practices as regular employees and that they do not constitute an unreasonable, elevated risk to the school.

Q: Student Employees – What are we doing to minimize the risks associated with employing students?

- ☐ Are we training them in our expectations for proper use of the school's information systems?
- ☐ Do we provide a second user account to these systems that requires a different user ID and password than their regular "student" account?
- ☐ Do we quickly close those work accounts when the student is no longer employed?
- ☐ Do student workers sign confidentiality and/or nondisclosure agreements?
- ☐ To what degree do we allow student volunteers to have access to critical applications?
- ☐ Are we training student volunteers and holding them to the same level of accountability as student employees?

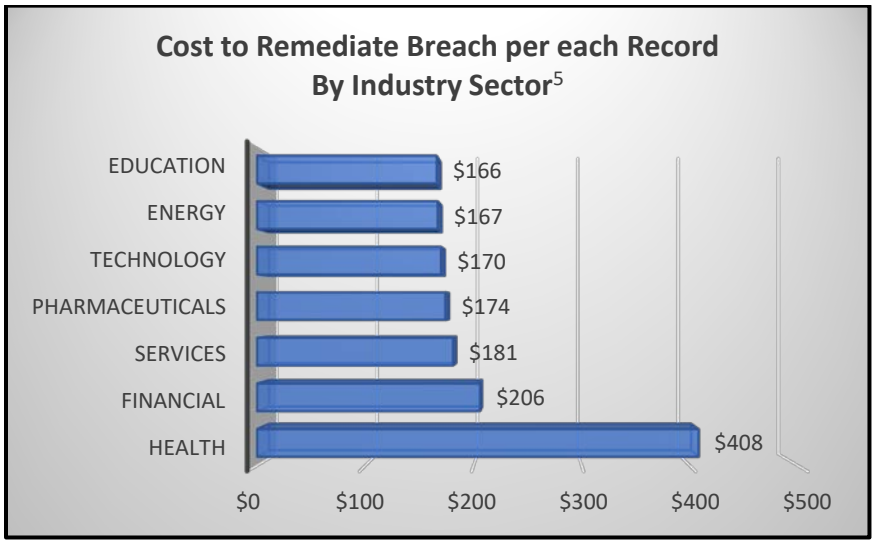
TOPIC: COST OF DATA BREACHES

Definitions:

- *Incident* – A security event that may have compromised the integrity, confidentiality or availability of an information asset
- *Breach* – An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party

In the 2018 Cost of a Data Breach Study: Global Overview, conducted by Ponemon Institute LLC, one factor found to affect the cost of a data breach was the unexpected loss of customers following a data breach. For a university, this equates to the loss of reputation and trust to attract new students. Program that preserve trust and loyalty in advance of a breach will help reduce the degree of abnormal churn. The loss of customer trust has serious financial consequences.

Another factor that should cause concern for all administrators is the cost to mitigate a data breach. According to a study by the Ponemon Institute[12], the average cost to remediate a breach across all industry sectors is $148 per individual record. The average cost per education record is $166 and $206 per financial record. And because many campuses have a student health component, there should be great interest in protecting health data. The average cost to resolve a health data breach is the highest at $408 per patient record as shown in the following table.



Some of the typical costs involved in remediating a breach are:

- Conducting investigations and forensics to determine root cause of the breach
- Determining the probable victims whose records were breached
- Conducting communication and public relations outreach
- Preparing notices to the victims and regulators
- Implementing call center procedures and specialized training
- Audit and consulting services
- Legal services for defense
- Free or discounted services offered to the victims
- Identity protection services

[12] "2018 Cost of a Data Breach Study: Global Overview," benchmark research sponsored by IBM Security and independently conducted by Ponemon Institute, LLC.

And none of the costs computed above reflect:

- The impact on the school's ability to provide federal student aid (for GLBA violations)
- The lost opportunities to attract or retain top students due to a damaged reputation
- Costs to rebuild the school's reputation and goodwill with students, parents and donors
- Or the fines that are usually levied by federal agencies and state attorneys general who seem to have found a new revenue stream

Q: Data Breaches – What have we done to prepare for a data breach?

- ☐ Do we have a cyber security insurance policy?
- ☐ Is there a properly trained forensic team in place that knows how to secure evidence?
- ☐ Is our legal counsel trained in addressing a data breach?
- ☐ Do we know our state's requirements for reporting breaches?
  - Timeliness requirements
  - Content of breach report
  - Official to whom breaches are reported
- ☐ Do we have a Data Breach Remediation Plan?
  - If so, does the plan address:
    - How to assess a breach for scope and vector
    - Notification to affected individuals
    - Notification to law enforcement
    - Notification to the media
    - Process to set up credit monitoring for affected individuals
- ☐ Do we need an unbiased, outside team to assess our vulnerabilities?

CLOSING THOUGHTS

As we have shown in this white paper, the measures needed to protect the privacy of information and the security of systems are varied, complicated and not without significant costs.

If you have been able to correctly and fairly adjudge your school's readiness by answering 90% or more of these questions in the affirmative, you may reasonably consider your "GPA" to be in the upper echelon of colleges and universities.

On the other hand, if you have reasonably concluded that you cannot answer many of these questions with a clear and resounding "Yes," your school has a lot of work to do!

About the author Joe D. Gillespie, MHS, RHIA, CHPS

Joe retired in 2017 after 13 years at the University of Kansas where he served in a dual role as the HIPAA Privacy Official for the Lawrence campus and as the Associate Director for Watkins Health Services. Joe was also an adjunct professor at the University of Kansas Medical Center as well as Johnson County (KS) Community College. Nowadays, Joe happily works part time as a Senior Privacy/Security Consultant for tw-Security where he continues to serve as a trusted advisor for his colleagues in academia and healthcare. ***Joe can be reached at joe.gillespie@tw-security.com***