AITS Enterprise Systems Assurance (ESA)
April 2014

MAINTAINING A PROPER SECURITY POSTURE IN HIGHER EDUCATION

PRIVILEGED AND CONFIDENTIAL – DO NOT DISTRIBUTE

EXECUTIVE SUMMARY

The potential for sensitive data breaches threatens the security of our organization.

Within Higher Education, the top 10 information technology breaches have resulted in 4.3 million sensitive records being unintentionally disclosed during the last eight years. Costs of a breach can include notification of those affected, forensics investigations to determine the cause and scope of compromise, identity theft protection services provided to those affected, loss of business and reputation, and remediation of the root cause of breach. In many cases sensitive information remains exposed to external attackers for years prior to being discovered and prevented by system owners.

Data breaches in higher education cost colleges an average of $111 per record according to a 2013 study published by the Ponemon Institute, which studies cybersecurity and data protection. Titled "2013 Cost of Data Breach Study: Global Analysis," the report included 277 organizations in nine countries and focused on breaches involving 1,000 to 100,000 records. The average total organization cost of data breaches for the Education industry is $3,192,915.

The University of Illinois has purchased breach insurance from Beazley at an annual cost of $384,500 with a limit of $10 million and a deductible of $500,000.

Illinois Pension Reform is another threat to the security of our organization. High turnover is inherently dangerous for areas responsible for sensitive data. Replacement employees bring about additional risk factors, including new access to large volumes of our organization's most sensitive information.

Statement of Findings and Recommendations

AITS Enterprise Systems Assurance (ESA) has compiled a summary of what we believe are gaps in our existing security posture, with deliberation for making the most of any resource investments. This report describes our rationale and conclusions.

Mitigation costs required for hardware and software tools are estimated to total $674,000 while additional staff resources are projected to total $350,000 annually for 5 FTE.

Threats/vulnerabilities that have recommended follow up actions are listed below. Detailed results can be found in later sections of this document.

- Targeted Email Attacks (Phishing)
- Multi Factor Authentication
- Scan for Sensitive Data
- Tighten Firewall Access
- Improved Data Practices
- Enhanced Contract Language
- Mobile Device Policy
- Formal Risk Assessment
- Enhance Workstation and Server Patch Process
- Enhance Monitoring
- Enhance Workstation and Server Anti-Virus Process
- Penetration Testing
- Non-Production Database Data
- Eliminate/Expire Sensitive Data from Systems

BACKGROUND INFORMATION

Recent Breaches in Higher Education

On February 18, The University of Maryland had one of their records databases compromised by external attackers. This particular database held information dating back to 1998 and includes names, Social Security numbers, dates of birth, and university identification numbers for 309,079 people affiliated with the school. The attackers did not alter data but made a copy of the information.

In response to the compromise, President Wallace Loh formed a task force to launch a comprehensive, top-to-bottom investigation of all computing and information systems. This included both central systems operated by University IT as well as edge systems operated by individual administrative and academic units. President' Loh's investigation called for three deliverables. First, every database would be scanned to identify the location of sensitive information, allowing migration or additional protection. Second, penetration tests would be performed on an ongoing basis. Third, the appropriate balance between centralized and decentralized IT systems would be reviewed to ensure uniform safeguards were in place.

Below, a study of the largest data breaches within higher education includes many other examples of similar activity (see Appendix I for more details).

Date Recognized	College or University Name	Records Exposed	Vulnerability Source
November 2006	University of California Los Angeles	800,000	Database Compromise
December 2010	Ohio State University	750,000	Server Compromise
May 2012	University of Nebraska	650,000	Database Compromise
February 2012	University of North Carolina Charlotte	350,000	Improper Storage
November 2008	University of Florida College of Dentistry	330,000	Server Compromise
February 2014	University of Maryland	300,000	Database Compromise
January 2012	Arizona State University	300,000	Server Compromise
May 2006	Ohio University	300,000	Server Compromise
March 2014	North Dakota University	290,000	Server Compromise
October 2012	Northwest Florida State College	279,000	Server Compromise
September 2009	University of North Carolina Chapel Hill	236,000	Server Compromise
November 2012	Western Connecticut State University	235,000	Database Compromise
February 2014	Indiana University	146,000	Improper Storage

While information related to the causes of these compromises has in many cases not been fully disclosed, it is still possible to make some helpful observations. The causes tend to fall within three broad categories: compromise of systems, compromise of credentials, and improper storage of sensitive data assets.

Another interesting observation is time to discovery. In many cases sensitive information remains exposed to external attackers for years prior to being discovered and prevented by system owners.

Costs Associated with a Breach

The effects of a breach can include the following direct and indirect costs:

- Notification of those affected
- Forensics investigations to determine the cause and scope of compromise
- Identity theft protection services provided to those affected
- Loss of business and reputation
- Remediation of the root cause of breach

Data breaches in higher education cost colleges an average of $111 per record according to a 2013 study published by the Ponemon Institute, which studies cybersecurity and data protection. Titled "2013 Cost of Data Breach Study: Global Analysis," the report included 277 organizations in nine countries and focused on breaches involving 1,000 to 100,000 records.

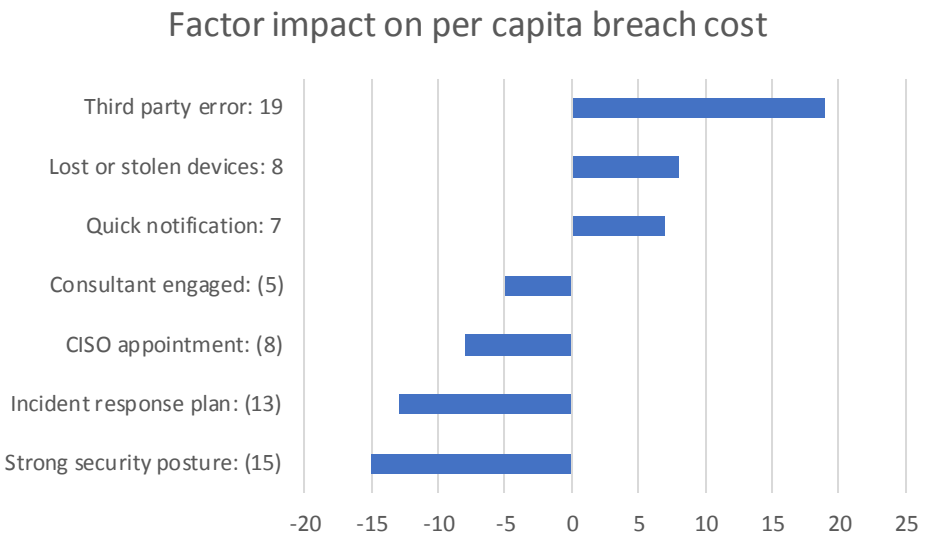
The study does not directly apply to catastrophic or mega data breaches because these are not typical of the breaches most organizations experience. On average, US companies had 28,765 exposed or compromised records during 2013. The average total organization cost of data breaches for the Education industry is $3,192,915.

The study identified seven factors that influence the cost consequences of a data breach incident. These attributes decrease the per capita cost of data breach:

- **The company had a relatively strong security posture at the time of the incident.** Organizations had a security effectiveness score (SES) at or above the normative average. We measured the security posture of each participating company using the Security Effective Score (SES) as part of the benchmarking process.
- **The company had an incident management plan.** Organizations had a data breach incident management plan in place at the time of the data breach event.
- **CISO (or equivalent title) has overall responsibility for enterprise data protection.** Organizations have centralized the management of data protection with the appointment of a C-level information security professional.
- **Consultants were engaged to help remediate the data breach.** Organizations engaged consultants to assist in their data breach response and remediation.

These attributes increase the per capital cost of data breach:

- **Data was lost due to third party error.** Organizations had a data breach caused by a third party, such as vendors, outsourcers and business partners.
- **The data breach involved lost or stolen devices.** Organizations had a data breach as a result of a lost or stolen mobile device, which included laptops, desktops, smartphones, tablets, servers and USB drives containing confidential or sensitive information.
- **The company notified data breach victims quickly.** Organizations notified data breach victims and/or regulators within 30 days after the discovery of data loss or theft.



Breach Insurance at the University of Illinois

The University of Illinois has purchased breach insurance from Beazley at an annual cost of $384,500 with a limit of $10 million and a deductible of $500,000. The maximum number of people that could be contacted based on a breach of confidential information is 3 million people. Some other sub-limits apply for public relations services. An internal response protocol is needed to enable timely response and engagement between the University and Beazley in the event of a claim.

The Security Effects of Illinois Pension Reform

Many features of the retirement programs administered by the State Universities Retirement System (SURS) may change on June 1, 2014 as a result of the enactment of Public Act 98-599, a comprehensive overhaul of public pension funding for the state of Illinois. These changes are expected to result in staff turnover, either through induced retirement for those eligible, or through resignations for those pursuing higher compensation opportunities.

High turnover is inherently dangerous for areas responsible for sensitive data. User credentials may exist in nuanced locations, resulting in untimely revocation of access. Operational knowledge of where sensitive data is being stored may be inadvertently lost due to lack of documentation or lack of adherence to standardized security practices. Replacement employees bring about additional risk factors, including new access to large volumes of our organization's most sensitive information, lack of familiarity with University data security policies, and security risks associated with new employee failure and departure.

MANAGING RISK

Higher education presents a unique challenge to securing data due to the nature of a University's edge-focused culture of loosely organized semiautonomous faculty and staff. A lack of central authority often results in an uneven landscape with respect to security policy compliance. The lack of common IT operational procedures such as change control, change management, patch management, and configuration management also inhibit reaching a uniform security level.

A common approach to addressing these challenges is to take a top-down approach to securing infrastructure and concentrate on core systems. Sensitive data should be migrated to central storage, and policies should be enforced for those that need to connect to core data. System security controls such as network segments can then be applied commensurate with the sensitivity of data being stored and commensurate with the levels of users' adherence to policies.

Stated differently, the University as a whole must focus on defining what comprises sensitive information assets and cataloging the locations where these assets are being stored. Existing countermeasures should be assessed to determine a baseline of controls for sensitive data. The goal of the institution is then to raise the level of these controls and ultimately to raise the level of the baseline for sensitive data in a way that is uniformly practiced by all system owners.

SENSITIVE DATA

The University works with the following types of sensitive data (see Appendix II for more details):

- Electronic Protected Health Information (ePHI)
- Social Security numbers (SSN)
- Payment Card Industry (PCI) data
- Automated Clearing House (ACH) data
- Intellectual Property
- Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- Fraud Transactions
- Toxic Chemicals (Weapons)

FORMAL RISK ASSESSMENT METHODOLOGY AND APPROACH

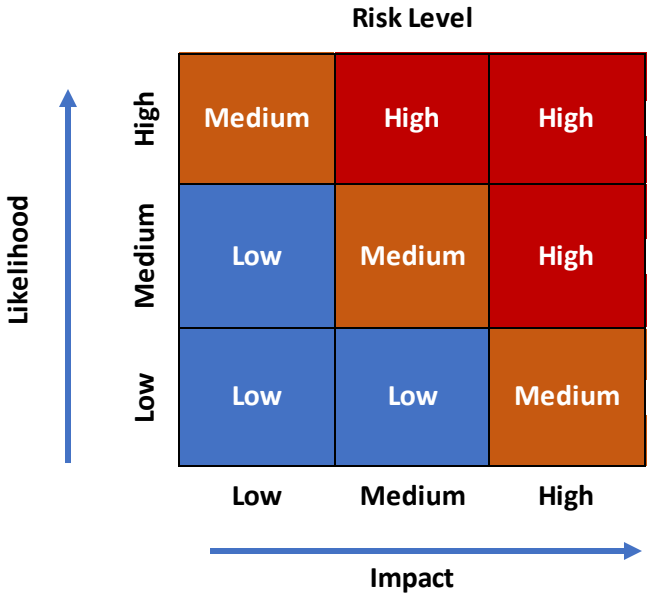
Within the University, every department in possession of sensitive data should undergo a formal risk assessment managed by an experienced assessor.

A risk assessment measures residual risk within an organization after considering the likelihood and impact of a particular vulnerability, and after considering existing controls that mitigate the risk. The organization's objective is then to either accept the risk or to recommend and prioritize further resources for mitigation.

Likelihood of a future adverse event is determined by analyzing threats to an IT system in conjunction with the potential vulnerabilities.

Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impact, and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data).

Controls are measures taken to avoid, counteract, or minimize security risks of an information system from attacks against the confidentiality, integrity, and availability of the information system.



Frameworks and standards for risk assessment are available from the National Institute of Standards and Technology (NIST), including NIST Special Publication 800-39: Managing Information Security Risk. Standards for controls are available from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) including ISO/IEC 27002. Additional control sets also include NIST SP 800, PCI-DSS, and publications from e.g. the SANS Institute and Information Systems Audit and Control Association.

The risk assessment methodology encompasses these steps:

1. Information Gathering
    a. Governance Policies
    b. Procedures and Practices
    c. Hardware
    d. Software
    e. Facilities
    f. Organization
2. Data Storage Identification
    a. Protected Health Information
    b. Sensitive Data
    c. Receives
    d. Processes
    e. Transports
    f. Stores
3. Threat/Vulnerability Identification Risk Evaluation
    a. Threats
    b. Vulnerabilities
    c. Likelihood
    d. Impact
    e. Risk of disclosure
        i. Unauthorized
        ii. Unintentional
        iii. IT interruption
        iv. Failure of due care
4. Risk Mitigation Evaluation
    a. Identification of existing controls
    b. Identification of potential controls
    c. Categorization of controls
    d. Best practices
        i. Information Privacy
        ii. Information Security
        iii. Healthcare information
5. Risk Assessment Risk Mitigation Strategy
    a. Residual Risk Scoring
    b. Acceptance of Residual Risk
    c. Plan of Risk Mitigation
    d. Prioritization of Risk Mitigation Steps

FINDINGS AND RECOMMENDATIONS

This section documents key threats/vulnerabilities, descriptions of their potential impact, controls in place, ratings for likelihood, potential impact, risk, recommendations for risk mitigation, and estimated costs for mitigation.

FINDING DETAILS ARE NOT INCLUDED IN THIS VERSION OF THE REPORT.

TO RECEIVE THE FULL, NON-REDACTED REPORT, PLEASE CONTACT AITS.

APPENDIX I. UNIVERSITY BREACH DETAILS

November 2006, University of California Los Angeles. Los Angeles California. 800,000 records. Database Compromise.

The University of California, Los Angeles warned students, parents, faculty and staff on Tuesday that they may be at risk of identity fraud after an unknown attacker breached a university-administered database containing personal information on approximately 800,000 people. The database--whose purpose was not described in UCLA's statements--contained names, Social Security numbers, dates of birth, home addresses and contact information, but not banking and credit-card information nor driver's license numbers, the university said in a statement published on Tuesday. The database contained information on the school's current students, faculty and staff, some former students and applicants as well as some parents of those students that applied for financial aid. The attacks occurred between October 2005 and November 2006, the university stated. The school took action on November 21, when network administrators noticed unauthorized activity, blocking further access to the database.

December 2010, Ohio State University. Columbus, Ohio. 750,000 records. Server Compromise.

750,000 current and former Ohio State University students, faculty and staff this week are being notified that their personal information was repeatedly compromised earlier this year by hackers who managed to access an unsecured university server. The breach, which was first discovered during a routine IT security review in late October, allowed the hackers to access student and staff files containing names, social security numbers, birth date s and addresses.

May 2012 University of Nebraska. Lincoln, Nebraska. 650,000 records. Database Compromise.

The University of Nebraska Peoplesoft student system was breached by a student hacker. A university technical staff member discovered a breach on May 23. Staff took steps to limit the breach and there was no clear evidence that any information was downloaded. The social security numbers, addresses, grades, transcripts, housing, and financial aid information for current and former University of Nebraska students may have been accessed. The database also included the information of people who applied to the University of Nebraska, but may have not been admitted, and alumni information as far back as the spring of 1985. Officials at the University of Nebraska in Lincoln (UNL) have identified an undergraduate student they say is responsible for a recent intrusion into a university database containing personal information on more than 650,000 students, parents and employees.

February 2012, University of North Carolina at Charlotte. Charlotte North Carolina.
350,000 records.
Improper Storage.

Confidential data, including bank account and Social Security numbers for some 350,000 University of North Carolina-Charlotte students, staff and faculty, were accidentally exposed -- some for almost 15 years -- due to a system misconfiguration and incorrect access settings that made electronic data publicly available. The school on Wednesday released a statement on an investigation it launched in February after staff discovered the data breach. The investigation revealed two separate incidents exposed data such as names, addresses, Social Security numbers and financial account information provided during university transactions. One incident involved misconfigurations and incorrect access settings made during a general university system upgrade that left data stored on the university's H: drive exposed on the Internet from Nov. 9, 2011 to Jan. 31, 2012. The second involved improperly stored sensitive data belonging to the school's College of Engineering that allowed for unauthorized access from 1997 until February 2012.

November 2008, University of Florida College of Dentistry. Gainesville, Florida.
330,000 records.
Server Compromise.

Some current and former dental patients have been notified that an unauthorized intruder recently accessed a College of Dentistry computer server storing their personal information. College information technology staff members were upgrading the server and found software had been installed on it remotely. Information stored on the server included names, addresses, birth dates, Social Security numbers and, in some cases, dental procedure information for patients dating back to 1990.

February 2014 University of Maryland. College Park, Maryland.
300,000 records.
Database Compromise.

The University of Maryland, located in College Town Maryland, had one of their records databases hacked Tuesday January 18, 2014 around 4:00 a.m. by an outside source. This particular database holds information dating back to 1998 and includes names, Social Security numbers, dates of birth and university identification numbers for 309,079 people affiliated with the school at their College Park and Shady Grove campuses. The hackers did not alter anything in the actual database, but apparently have made a "copy" of the information. The university commented at how sophisticated the attack was by the hacker or hackers and they must have had a "very significant understanding" of how the database was designed and maintained, including the level of encryption and protection of the database.

January 2012, Arizona State University. Tempe, Arizona.
300,000 records.
Server Compromise.

On Wednesday evening, ASU students and employees were told in a security text alert that the university's ASURITE computer system may have been compromised and that all online services had been suspended. This is the university's main online system, where students and employees put in their passwords to log in and access classes and other services. More than 300,000 people have accounts through the system. ASU officials said an encrypted file containing user names and passwords was downloaded Wednesday by an unknown person outside the university. There is no evidence that any information has been compromised, but all online services were shut down as a precaution.
ASU Video:
http://www.statepress.com/2012/01/24/students-and-faculty-speak-out-against-asu-hacking/

May 2006, Ohio University. Athens, Ohio.
300,000 records.
Server Compromise.

Ohio University's database has been compromised for over a year, and hackers have had access to the personal data of more than 300,000 alumni and other people. Included in this data are 137,000 Social Security numbers. Ohio University President Roderick McDavis announced at a press conference Monday that he, too, is among the more than 300,000 alumni and friends of Ohio University - not current students - whose personal information may have been compromised when unauthorized access was gained to a computer system supporting alumni relations.

March 2014, North Dakota University. Bismarck, North Dakota.
290,000 records.
Server Compromise.

North Dakota University System has notified individuals of a security breach of a computer server that stores personal information on students, staff and faculty. On February 7, 2014 the server was hacked into and more than 209,000 current and former students and 780 faculty and staff had personal information stored on thus server that included names and Social Security numbers according to Larry Skogen, the Interim Chancellor. The university has notified officials and has set up a website www.ndus.edu/data with information and is organizing a call center for questions from those who were affected. Authorities have announced that "an entity operating outside the Unites States apparently used the server as a launching pad to attack other computers, possibly accessing outside accounts to send phishing emails".

October 2012, Northwest Florida State College. Niceville, Florida.
279,000 records.
Server Compromise.

The employee data was breached between May 21 and Sept. 24 after one or more hackers accessed a folder on the school's main server. According to school officials, an internal review between Oct. 1 and Oct. 5 revealed that 76,000 current and former students of Northwest Florida State College (NWFSC) had their personal information exposed in the bre ach, as did approximately 200,000 students from Florida who were eligible for the Bright Futures scholarships for the 2005-2006 and 2006-2007 school years. In addition, more than 3,000 current and retired employees had their information exposed as well.

September 2009, University of North Carolina, Chapel Hill. Chapel Hill, North Carolina.
236,000 records.
Server Compromise.

A hacker has infiltrated a computer server housing the personal data of 236,000 women enrolled in a UNC-Chapel Hill research study. Among the information exposed: the Social Security numbers of 163,000 study participants. Though the intrusion was detected in late July, computer forensics experts say it may have happened two years ago, said Matthew Mauro, chairman of the UNC-CH Department of Radiology. And though UNC-CH officials and a private computer forensic expert have spent two months investigating, they still don't know who did the hacking, where the attack originated, or even whether data was downloaded.

November 2012 Western Connecticut State University. Danbury, Connecticut
235,000 records.
Database Compromise.

A computer vulnerability allowed the information of students, student families, and other people affiliated with the University to be exposed. The records covered a 13 year period and included Social Security numbers. High school students who had associations with the University may have had their SAT scores exposed as well. The issue existed between April 2009 and September 2012.
Configuration controls on a general database at the university were incorrectly set, which could have allowed an outsider to remotely access the data contained within. The misconfiguration was discovered during routine maintenance. It had existed from April 2009 to September of this year.

February 2014, Indiana University. Bloomington, Indiana.
146,000 records.
Improper Storage.

Indiana University announced that the personal data of 146,000 students and graduates was breached. The information included their Social Security numbers and addresses and may have affected students and graduates from 2011 to 2014 at seven of its campuses. According to the university "The information was not downloaded by an authorized individual looking for specific sensitive data, but rather was accessed by three automated computer data-mining applications, called webcrawlers, used to improve Web search capabilities." The university also announced that the information was stored in an insecure location for the past 11 months. The site has since been locked down.

APPENDIX II. TYPES OF SENSITIVE DATA

Electronic Protected Health Information (ePHI)

ePHI is "individually identifiable" "protected health information" sent or stored electronically. Protected health information refers to items such as:

- An individual's past, present, or future physical or mental health or condition
- The past, present, or future provisioning of health care to an individual
- The past, present, or future payment-related information for the provisioning of health care to an individual

"Individually identifiable" means information that can be linked back to a specific individual (even if this is indirect). There are 18 types of identifiers for an individual (listed below). Any of these, combined with some kind of "protected health information" (e.g. an appointment with a particular doctor) would constitute ePHI.

Name, Address, All elements of dates related to an individual, Telephone numbers, Fax number, Email address, Social Security number, Medical record number, Health plan beneficiary number, Account number, Certificate/license number, Any vehicle or other device serial number, Device identifiers or serial numbers, Web URL, Internet Protocol (IP) address numbers, Finger or voice prints, Photographic images, Any other characteristic that could uniquely identify the individual

Social Security numbers (SSN)

The Social Security Number (SSN)'s primary purpose is to identify employees in payroll systems to ensure they are making proper tax and other deductions, and by the Internal Revenue Service for taxation purposes. The SSN has become a universal identification number used for many purposes around the country.

Payment Card Industry (PCI) data

The Payment Card Industry Data Security Standard (PCI-DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI-DSS provides a baseline of technical and operational requirements designed to protect cardholder data which includes:

Primary Account Number (PAN), Cardholder Name, Expiration Date, Service Code

Automated Clearing House (ACH) data

Automated Clearing House (ACH) is a secure payment transfer system that connects all U.S. financial institutions. The ACH network acts as the central clearing facility for all Electronic Fund Transfer (EFT) transactions that occur nationwide, representing a crucial link in the national banking system. ACH Protected Information is defined as the non-public personal consumer information, including financial information, such as:

Name, Physical Address, Phone Numbers, Email Addresses, Account Numbers, Invoice Numbers, Social Security Number, Driver's License Number, Business ID Number, Types and amounts of transactions.

Intellectual Property

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR)

The International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) are two important United States export control laws that affect the manufacturing, sales and distribution of technology.

The legislation seeks to control access to specific types of technology and the associated data. Its goal is to prevent the disclosure or transfer of sensitive information to a foreign national.

Fraud Transactions

Toxic Chemicals (weapons)

APPENDIX III. INDIANA UNIVERSITY BREACH RESPONSE COSTS

Data breach response costs IU more than $80,000

The Associated Press

BLOOMINGTON, Ind. -- Indiana University says it has spent more than $80,000 responding to a computer data breach that exposed personal information of some 146,000 current and former students.

The university reported last month that information including names, addresses and Social Security numbers of those who attended any of the university's campuses from 2011 to 2014 was unsecured for more than 11 months because security protections weren't working correctly.

An investigation hasn't yet turned up evidence that any information has been compromised or improperly used, university spokesman Mark Land told The Herald-Times (http://bit.ly/1kWrJ0T)

A call center number (866-254-1484) set up for questions about the data breach will remain active through at least this week, Land said. It has received about 950 calls so far, with roughly half coming on the first day.

About 700 personnel hours by IU employees have been spent so far on its response, Land said.

IU officials believe that no outside person had accessed the encrypted data. The information was immediately secured, and officials are looking at all processes to make sure that it doesn't happen again, Land said.

He said three "web crawlers," or data-mining applications, had accessed the data. The crawlers were one for Google, one for a search engine that no longer exists and one for Baidu, a Chinese search engine, he said. Land said Google has since cleared the information.

University officials notified all those involved, primarily by email, Land said. About 6,200 people didn't have emails on file with the university, so IU spent more than $6,000 to mail out letters.

The call center was contracted by the university at $75,000, he said.

APPENDIX IV. SANS TOP 20 CRITICAL SECURITY CONTROLS

Critical Security Controls for Effective Cyber Defense

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In 2008, this was recognized as a serious problem by the U.S. National Security Agency (NSA), and they began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe. Ultimately, recommendations for what became the Critical Security Controls (the Controls) were coordinated through the SANS Institute. In 2013, the stewardship and sustainment of the Controls was transferred to the Council on CyberSecurity (the Council), an independent, global non-profit entity committed to a secure and open Internet.

The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. The actions defined by the Controls are demonstrably a subset of the comprehensive catalog defined by the National Institute of Standards and Technology (NIST) SP 800-53. The Controls do not attempt to replace the work of NIST, including the Cybersecurity Framework developed in response to Executive Order 13636. The Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.

Top 20 Critical Security Controls - Version 5

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services

12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises