GREENE ACADEMY CASE STUDY

Georgia Southern University
Aleigha Daniels, Kacey Smith, Blaine Geiger, Stuart Collins, Gavin Glass

1. Data Classification Standards & Risk Awareness Methodology (Aleigha Daniels)

A. Data Classification:
Data classification standards are policies an organization uses to classify data. Data classification in four categories:

- Private data: data that requires privacy protection.
- Confidential: the organization owns the information.
- Internal use only: information shared within an organization, not intended to leave the organization.
- Public domain: data imparted to the public.

In order to maintain student privacy, Greene Academy should adhere to the Family Educational Rights and Privacy Act (FERPA) standards. FERPA governs the privacy of student educational records. Personal information, educational data, and directory information are all collected under FERPA. Personal information is private data only disclosed to the students and parents. Educational data is for internal use only within the academy. Directory information is public data is not considered harmful. In accordance with FERPA, schools must obtain written consent from parents or eligible students before disclosing personal information.

B. Risk Awareness Methodology:
For risk assessment, both NIST SP 800-30 revision 1 and OCTAVE Allegro are valid options. With NIST SP 800-30 revision 1 being more comprehensive and structured, the risk assessment Greene Academy will focus on will be the OCTAVE Allegro version, the more concise version of OCTAVE. With limited resources and expertise in risk management, OCTAVE Allegro is more appropriate. It offers a self-directed approach and is designed for smaller and medium-sized businesses. A workshop-based approach is to gather both information and to make decisions. When considering the relationship between people, technology, facilities, business processes, and the services they support, OCTAVE Allegro takes a holistic view. OCTAVE Allegro steps include:

- Step 1: Establish Risk Measurement Criteria
- Step 2: Develop an Information Asset Profile
- Step 3: Identify Information Asset Containers
- Step 4: Identify Areas of Concern
- Step 5: Identify Threat Scenarios
- Step 6: Identify Risks
- Step 7: Analyze Risks
- Step 8: Select Mitigation Approaches

Using OCTAVE Allegro, organizations can analyze information-based assets without the need for a lot of resources.

Caralli, R. A., Stevens, J.F., Young, L. R, & Wilson, W.R. (2007, May). Introducing Octave Allegro: Improving the information security risk ... Software Engineering Institute. https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf

Family educational rights and privacy act (FERPA). US Department of Education. (2021). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Ferpa-protected data. Long Beach City College. (2019). https://www.lbcc.edu/post/ferpa-protected-data

Hlavac, G. C., &Easterly, E. J. (2015). Ferpa Primer: The basics and beyond. NACE. https://www.naceweb.org/public-policy-and-legal/legal-issues/ferpa-primer-the-basics-and-beyond/

Kim, D., & Solomon, M. G. (2021). Fundamental of Information Systems Security (4th ed., p.313). Jones & Bartlett Learning.

Rivera, R. (n.d). Comparison of OCTAVE and NIST's Special Publication 800-30 Methodologies. Angelfire. https://www.angelfire.com/tx5/techpc/Octave.html

Caralli, R. A., Stevens, J.F., Young, L. R, & Wilson, W.R. (2007, May). Introducing Octave Allegro: Improving the information security risk ... Software Engineering Institute. https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf

1. Gap Analysis (Blaine Geiger)

A. Research into Gap Analysis Plans:

In a broad sense, the approach, planning, and methods of gap analysis that various security professionals adhere to will always include some basic steps in common. Basic steps for gap analysis may include the following:

- Identify relevant security policy elements and standards.
- Compile policy, standard, procedure, and guideline documents.
- Evaluate the implementation of these documents.
- Gather hardware and software inventory information.
- Assess user awareness and adherence to policies through interviews.
- Compare current security practices with established policies.
- Prioritize and address security gaps.
- Document and execute solutions to align with policies.

Resources have varying levels of detail included in the plans and methods they suggest. Some online resources such as the ISACA provide a basic framework for gap analysis planning. These guidelines, like those above, contain similar steps. The steps here are comparable to other resources, but their organization and conciseness is a great example of gap analysis planning and methods:

- Identifying an appropriate security framework: Choose an acknowledged security standard like ISO/IEC 27002 as a benchmark. These industry standards have been proven most effective and provide a basis for comparison to your organization's current security controls and policies.
- Examine staff/people and processes: performing in-depth investigation into the impact people have in the organization's security. Including effectiveness of staff training, system access methods, and practices for executing changes across the organization.
- Data gathering: Compile and examine data to determine how current security measures are performing in context of the present system.
- Perform a thorough assessment of the overall security program. You should identify strengths and weaknesses of the current system. Develop suggestions and strategies for necessary improvements.

B. Scope

The scope of the gap analysis project includes a comprehensive assessment of the entirety of all technological aspects of Greene Academy and its information systems. Faculty, staff, students, IT personnel, stakeholders, and all roles/users of the system as it relates to system security are within the scope of this analysis. The focus of the project is to bring the organization's security into closer alignment with industry standards and best practices, while achieving the needs decided upon and remaining within constraints. In addition, the project's scope encompasses the development of forward-looking strategies to prepare for future challenges.

C. Constraints

There are several identified constraints that may influence project outcomes. The budgetary cap of $400,000 for initial expenses and $50,000 for annual maintenance will require careful consideration of financial planning. The personnel constraints are of significance. With the budget for one IT Security Manager and two Network Security Administrator/Technicians. It is crucial to ensure these positions are filled by people with the expertise to perform as much of the gap analysis and implementation as possible. If not, anything they cannot perform may lead to higher expenditures in consulting costs for someone qualified, affecting the budget.

Personnel and technological constraints can be influenced by budgetary constraints. For example, if an entire system requires replacement, this may not be feasible due to budgetary constraints. Technological constraints may also be purely due to technological impossibility. For instance, a legacy system which will certainly be a technological constraint may be completely incompatible with a particular security solution. This solution would not work due to the incompatibility, regardless of the cost or budget.

D. High-Level Plan to Perform Gap Analysis

Define IT security goals for Greene Academy by focusing on present security measures related to access controls, level of security awareness of users, development of comprehensive security policies, network connectivity protection, internet access and security, email security both internal and external, shared information storage security, and remote access security. This applies to all computers in the lab, offices, classrooms, and teachers accessing documents and grades via remote access.

The present status of security controls at Greene Academy is severely lacking. The following is a list of security goals along with the suggested security controls to consider:

- Access controls - strong access policies, multi-factor authentication, role-based access, least privileges, auditing and access logs, access control lists, directory services.
- SETA - regular training and retraining sessions, security awareness campaign, development of any required education for integration of changes.
- Policies - establish IT security policy governance board, at minimum data protection and privacy, acceptable use, network security, email security, password management, and remote access policies apply to security gaps at Greene Academy. Further and complete IT security policy development is needed as well.
- Network connectivity protection - firewall, intrusion detection and prevention systems, network segmentation,
- Internet access security - antivirus, antimalware, content filtering, VPN, maintain patches and updates, SETA, two-factor authentication
- Email security - encryption, enhanced filtering, attachment scanning, access controls, SETA
- Shared information storage security - access controls, encryption, data backups, audit trails and logs, secure file transfer, physical security controls for central data storage.
- Remote access security - VPN, MFA, access controls and secure remote desktop protocols, SETA, secure file transfer

Given these possible solutions, each solution must be carefully evaluated as they compare to implementation, budgetary, and technological feasibility. Prioritize solutions that provide the most benefit in relation to cost. After solutions have been chosen an implementation plan should be drafted. The conclusion of the gap analysis will begin a transition into implementation.

Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (3rd ed., p.255). Burlington, MA: Jones & Bartlett Learning.

Ghaznavi-Zadeh, R. (2018). Information Security Architecture: Gap Assessment and Prioritization. *Information Systems Audit and Control Association (ISACA) Journal,* March 2018. Retrieved October 22, 2023, from https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/information-security-architecture-gap-assessment-and-prioritization#:~:text=Perform%20a%20gap%20analysis%20and,Architecture%20Framework%20and%20Gap%20Assessment

Sell, C. How To Conduct An Information Security Gap Analysis (2015). Retrieved October 22, 2023, from https://www.cio.com/article/251153/how-to-conduct-an-information-security-gap-analysis.html

2. Functional Information Security Policies (Kacey Smith)

A. Fair and Responsible Use of iPhones Provided by Greene Academy

1. Statement of Policy
    a. Scope and applicability - This policy applies to any authorized user of iPhones provided by Greene Academy, including all faculty, staff, students, and all other affiliates of Greene Academy.
    b. Definition of technology addressed - iPhones are any smartphone, operating with the iOS operating system, and all software and hardware on the device.
    c. Responsibilities - Users are responsible for using devices for intended purposes and maintaining the security and integrity of the device.

2. Authorized Access and Usage of Equipment
    a. User access - Access to iPhones is restricted to authorized users designated by Greene Academy.
    b. Fair and responsible use - Users are expected to utilize the iPhones for educational and professional purposes only, following ethical and legal guidelines.
    c. Protection of Privacy - Users must respect the privacy of others and refrain from unauthorized access to personal information.

3. Prohibited Use of Equipment
    a. Disruptive use or misuse - The iPhone provided by the organization will not be used to access prohibited sites nor to access or distribute harmful, offensive, or inappropriate material.
    b. Criminal use - Any use of the iPhone for illegal activities is strictly prohibited.
    c. Offensive or harassing materials - Users must not engage in the creation or distribution of offensive or harassing materials.
    d. Copyrighted, licensed, or other intellectual property (IP) - Users are prohibited from violating copyright or intellectual property laws.
    e. Other restrictions - Any other specific restrictions deemed necessary for the secure and responsible use of iPhones provided by Greene Academy.

4. Systems Management
    a. Management of stored materials - Users are responsible for managing and safeguarding the information stored on their iPhone.

b. Employer monitoring – Greene Academy reserves the right to monitor iPhone usage for security and compliance purposes.
c. Virus protection - Users must install and regularly update antivirus software to protect against malicious software.
d. Physical security - iPhones must be physically secured to prevent theft or unauthorized access.
e. Encryption - Users are encouraged to use encryption methods to protect sensitive data being sent or recieved.

5. Violations of Policy

a. Procedures for reporting violations - Violations should be reported to the designated IT support or security contact.
b. Penalties for violations - 1st Violation: Verbal/written warning and mandatory security training. 2nd Violation: Temporary suspension of iPhone privileges and additional training. 3rd Violation: Permanent revocation of iPhone privileges and disciplinary action, which may include academic or employment consequences.

6. Policy Review and Modification

a. Scheduled review of policy procedures for modification - The policy will be reviewed annually or as needed.
b. Who performs the reviews? - The IT department, in collaboration with relevant stakeholders, will conduct policy reviews.
c. Date of last review – 11/17/2023

B. Fair and Responsible Use of Email Provided by Greene Academy

Statement of Policy

a. Scope and applicability - This policy applies to any authorized user of email provided by Greene Academy, including all faculty, staff, students, and all other affiliates of Greene Academy.
b. Definition of technology addressed - The technology addressed includes email services and associated communication tools provided by Greene Academy.
c. Responsibilities - Users are responsible for utilizing email services for legitimate and authorized purposes, maintaining the security of their accounts, and respecting the privacy of others.

2. Authorized Access and Usage of Equipment

a. User access - Access to email services is granted only to authorized users designated by Greene Academy.
b. Fair and responsible use - Users are expected to use email for professional and educational communication in accordance with ethical and legal standards.
c. Protection of Privacy - Users must respect the privacy of others and refrain from unauthorized access to or disclosure of sensitive information.

3. Prohibited Use of Equipment

a. Disruptive use or misuse - Email services shall not be used for disruptive purposes or any activity that interferes with the normal operation of Greene Academy's communication systems.
b. Criminal use - Any use of email for illegal activities is strictly prohibited.
c. Offensive or harassing materials - Users must not engage in the creation or distribution of offensive or harassing materials.
d. Copyrighted, licensed, or other intellectual property (IP) - Users are prohibited from violating copyright or intellectual property laws in their email communications.
e. Other restrictions - Any additional specific restrictions deemed necessary for the secure and responsible use of email.

4. Systems Management

a. Management of stored materials - Users are responsible for managing and protecting the information stored in their email accounts.
b. Employer monitoring - The organization reserves the right to monitor email usage for security and compliance purposes.
c. Virus protection - Users must follow recommended security practices to protect email accounts from viruses and malware.

d. Physical security - Users should take measures to secure their devices to prevent unauthorized access to email accounts.
e. Encryption - Users are encouraged to use encryption methods for sensitive email communications.

5. Violations of Policy
    a. Procedures for reporting violations - Violations should be promptly reported to the designated IT support or security contact.
    b. Penalties for violations – 1st Violation: Verbal/written warning and mandatory security training. 2nd Violation: Temporary suspension of email privileges and additional training. 3rd Violation: Permanent revocation of email privileges and disciplinary action, which may include academic or employment consequences.

6. Policy Review and Modification
    a. Scheduled review of policy procedures for modification - The policy will be reviewed annually or as needed.
    b. Who performs the reviews? - The IT department, in collaboration with relevant stakeholders, will conduct policy reviews.
    c. Date of last review – 11/17/2023

3. Malware Attack and Security Breach (Gavin Glass)

A. Possible Reasons for the Attack and Security Breach:

There are many possible causes that could have led to this attack, and these are the same factors that can lead to a future attack. To address this issue, we need to look at the systems in place and the constraints that could lead to the breach. From a quick glance there are some causes that has resulted in this incident such as:

- The lack of Formal Security Policies
- Limited amount of Network Protection
- Insufficient amount of Security Education and Training
- Insufficient Email and Internet Security
- Lack of Information Storage Protection
- Lack of Restrictions on faculty, staff, and student computer uses

What insights about risks, threats, and vulnerabilities can you glean from reports of
similar incidents that have occurred in other organizations?
Malware Attacks and Security Breaches have been around for a long time and often follow similar paths to breaching security. Some online resources such as Kaspersky provide a basic understanding of what Breaches are and what are often the cause of them. These causes, like those above, had also occurred with Sony Pictures. Muyuan Li coves the case study of the massive data breach that occurred in late 2014:

- Through the use of Malware in both incidents like Greene Academy and Sony Pictures there were major security flaws that led to security vulnerabilities.
- In the Greene incident, the academy lacked dedicated protection for email and internet connectivity.
- The academy also had a limited information storage protection leaving sensitive documents and grades at risk for unauthorized access.
- In the Sony incident, Sony failed to maintain security countermeasures/policies, having something like the company's email retention policy left up to seven years of old encrypted messages on the company’s servers.
- Major lack of Email Security: Sony had long-term use of Email as a storage for business records, contracts, and documents.

- Lack of Formal Security Policy: Sensitive information such as IT Usernames/Passwords were stored on encrypted spreadsheets and Word files titles with names such as “Computer Passwords”.

B. Outcomes and Countermeasures

As for what the company should expect for Outcomes of the security breach, there can be expected Intellectual property exposure, such including student and faculty data. Another outcome to be expected is the disruption of normal operations, this affecting classes and administrative functions. The last major outcome is the damage of the Academy’s reputation as the trust in their security has been compromised.

There are many countermeasures that could be used to prevent such data breaches. These are some examples of countermeasure that could be used:

Implementation of Formal Security Policies:

- What it will do: Establish clear guidelines for secure behavior, defining acceptable use policies, and specifying security measures.
- Concerns: Resistance from faculty or staff, the need for ongoing updates to policies.

Network Intrusion Detection and Prevention Systems (NIDS/NIPS):

- What it will do: Monitor network traffic for suspicious activities and automatically block or alert administrators to potential threats.
- Concerns: False positives, potential impact on network performance.

Security Awareness Training Program:

- What it will do: Educate faculty, staff, and students about cybersecurity best practices, reducing the likelihood of falling victim to social engineering attacks.
- Concerns: Resource-intensive, ongoing effort required for effectiveness.

Email Filtering and Web Security Solutions:

- What it will do: Protect against phishing attacks, malware distribution through email, and malicious websites.
- Concerns: False positives, potential impact on legitimate communications.

Data Encryption for Information Storage:

- What it will do: Ensure that stored information is encrypted, adding an additional layer of protection against unauthorized access.
- Concerns: Implementation complexity, potential performance impact.

How Data Breaches Happen. *Kaspersky resource-center*. Retrieved November 15, 2023, from https://usa.kaspersky.com/resource-center/definitions/data-breach

Li, M. The Sony Pictures Entertainment Hack Case Report (2018). Retrieved November 16, 2023, from https://medium.com/@muyuanlii/the-sony-pictures-entertainment-hack-case-report-195c4681bf72

Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (3rd ed., p.78). Burlington, MA: Jones & Bartlett Learning.

4. Information Security Awareness Program (Kacey Smith)

A. Implementing a SETA Element:

The information security awareness program at Greene Academy is of utmost importance and should begin immediately. Allocating several weeks to comprehensive training sessions encompassing new policies, procedures, and best practices will be the cornerstone of this initiative, coupled with ongoing refresher training sessions tailored specifically for the faculty. The primary objective is to educate all members of the organization, with a heightened focus on departments handling sensitive information, such as office staff and senior personnel including the headmaster and department heads. Employing a diverse range of training methods is essential to ensure broad coverage and comprehension among all individuals.

It is imperative that the program targets the entire organization as the ubiquitous use of technology in today's world makes anyone within the organization susceptible to potential cyber threats. A malicious attack on any member can have far-reaching consequences for Greene Academy, especially if it compromises the network. While comprehensive training is crucial for everyone, a more specialized and in-depth approach is warranted for higher-level employees and those in specific departments dealing with sensitive information, given the increased likelihood of them being targeted.

Commencing with a dedicated week of presentations, videos, and online modules will provide a foundational understanding of new policies, procedures, and best practices for all faculty and staff. This foundational training will be followed by more intensive sessions tailored for high-ranking staff and others handling sensitive data. These sessions will emphasize the critical importance of cybersecurity and familiarize participants with the tools the organization employs, fostering a heightened awareness and providing a reference point within each department. Subsequently, the remainder of the organization will undergo e-training, with faculty leading the way to serve as a resource for students and other members seeking clarification.

The phased approach to training aims to create a cascading effect of awareness, where early education for faculty will facilitate a smoother dissemination of information throughout the organization. By raising awareness and providing comprehensive education, the organization anticipates a reduction in security incidents and an overall improvement in the security of data and information. This strategic implementation plan is designed to empower every member of Greene Academy to contribute actively to the protection of the organization's digital assets.

"CISA Cybersecurity Awareness Program | CISA." Cybersecurity and Infrastructure Security Agency CISA, 2021, www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program#:~:text=The%20CISA%20Cybersecurity%20Awareness%20Program,have%20a%20part%20to%20play. Accessed 17 Nov. 2023.

"Security Education Training and Awareness (SETA) – IT Living Lab." Livlab.org, 2023, livlab.org/seta/. Accessed 17 Nov. 2023.

5. Contingency Planning (Stuart Collins)

A. Incident Response Planning

INCIDENT – Virus Attack

A. Preparation

1. We will respond to this incident by:

- Identifying the threat and its legitimacy.
- Isolating and containing the threat.
- Eliminating the threat
- Restoring the system to its normal operating state.

2. The Incident Response Team (IRT) will consist of an incident team leader, a communications team leader, and the IT and IT security personnel. The IRT will be the head of the IT department, the two full-time technological support administrators, and other faculty or new-hire candidates with expertise in related fields. These personnel should receive training at regular intervals.

B. Triage

1. This is an incident if it threatens the security or operation of normal processes for a system in the network or the network itself.
2. The initial notification was received by the Incident Response Team via an alert from their security software.
3. This is a high priority incident because the virus could make its way onto other clients in the system and spread infection.

C. Notification

1. The first person to receive the notification should be a high-ranking member of the IRT, ideally the team leader or communication team leader. They should then notify the rest of the response team and any other necessary faculty to respond to the incident.
2. The first responder will use the security software to run diagnostics and determine if there is a real virus in the system or if the system had a "false positive".
3. After the legitimacy of the threat is validated and its scope has been determined, the IRT member will escalate. The rest of the IRT and other relevant staff members will be informed.

D. Response & Recovery

1. The incident will be contained by isolating the affected system(s) and disconnecting them from the network even if it requires physically unplugging the system.
2. The source of the incident was a student that unknowingly accessed malware on one of the computer lab computers.
3. The exploited vulnerability was a weakness in installed software due to a software vulnerability.
4. The recovery of any compromised data will take place on all affected computers after a full scan of the system and the replacement media.

E. Documentation and Reporting

1. The entire process of incident response should be documented. A member of the IRT will record the steps of the process including the actions taken that were ineffective as well as the effective ones.
2. The documentation should be written by a member of the IRT communication team member. It should be kept on a physical drive as well as stored within the cloud. The documents should be disseminated among the IRT as well as to members of the faculty to help prevent similar situations and improve the response to them if they do occur.

B. Business Continuity Planning

Critical Business Function (CBF)	Access to Class Content

Maximum tolerable downtime (MTD)	48 hours
Recovery Point Objective (RPO)	All files related to current assignments should be recovered or redistributed resulting in no loss of data.
Recovery Time Objective (RTO)	24 hours

Critical Business Function (CBF)	Student Grade Records
Maximum tolerable downtime (MTD)	1 week
Recovery Point Objective (RPO)	Student grades should be backed up both digitally and recorded physically while the function is down, for a RPO of 100%
Recovery Time Objective (RTO)	1 week

C. Disaster Recovery Planning

Potential Disaster: Hurricane

We will use a warm site in Knoxville, TN, because it is a major city with strong infrastructure and is much farther inland to prevent damage from the hurricane so that critical processes can be protected after being reestablished. We would place our EOC nearby but further inland in Alpharetta, GA. This way it could be reached quickly when necessary and would provide a safer place to orchestrate the DRP. Strategies we will use to continue processes in the interim consist of switching to remote learning until normal in person processes resume.

Disaster Recovery Planning Timeline.	
Time since incident	**Event (what your organization is doing)**
0 Hour	Detection of the disaster. Notify all personnel that the DRP is going into effect. Notify all students, and immediate family about the disaster and about the steps being taken.
1 Hours	Suspend in person classes and inform student to take the necessary safety precautions such as remaining safe in their dormitory or going back home to their families if available.
2 Hours	Ensure that students and faculty are taking the recommended safety precautions by working with the local law enforcement and working in tandem with emergency safety procedures.
3 Hours	Pack up all hardware containing critical data or essential to proper function and begin moving them to the warm site.
12 Hours	Begin re-establishing critical processes at the warm site in Knoxville, TN.

24 Hours	Complete setup of the warm site and re-establish limited functions.
48 Hours	Begin repairing and returning operations to the primary site.
1 Week	Re-establish full function on the primary site.

I believe that the disaster recovery would take a week as long as there is no cataclysmic damage to the Academy's structure. With a warm site in Knoxville, TN we should be able to begin setting up re-establishment of processes at a limited capacity within 12 hours of evacuation procedures. This timeline accounts for the regular 4-hour journey from Greene Academy to the warm site, as well as taking into consideration outside factors such as traffic or detours. After 24 hours, the warm site should be completely functional. After the disaster has passed, which I estimated to be the 36–48-hour mark repairs most likely must be made. However, if the repairs are not extreme then I believe that after one-week regular operation could resume at the primary site. This is likely to differ based on the severity of the hurricane in question.

Cerrigione, C. Incident Response Plan. (2015). Retrieved November 12, 2023 from https://security.uconn.edu/incident-response-plan/

Kim, D, & Solomon, M. (2023). *Fundamentals of information systems security* (4th ed.,p 371-388) Burlington, MA: Jones & Bartlett Learning.