SIR0020348

Incident Report

First Published: April 16, 2019
Last Updated: September 13, 2019
Handler: Nate Lewis
Report authors:

Jimmy Lummis, Chief Information Security Officer
Christopher Craig, Associate Director – Cyber Security
Kyle Koza, Principal Information Security Engineer
Nate Lewis, Information Security Operations, Senior

Cyber Security
Georgia Institute of Technology

Table of Contents

Summary

Beginning in December 2018, a malicious party used a SQL Injection attack against a financial aid web application resulting in the unauthorized disclosure of approximately 1.3 million records of personally identifiable information (PII). Impacted individuals include current and former faculty, students, and staff as well as applicants and others. This resulted in a yet to be determined financial impact to the Institute of at least $10,000, but likely to be much greater. At the time of writing, the incident is still being investigated by the FBI.

Background

On March 21st, 2019 the Enterprise Information Systems (EIS) department within Georgia Tech Information Technology identified this SQL Injection vulnerability in an internally developed financial aid application (GT App) while investigating a performance problem. Upon identifying the vulnerability, the development team implemented a patch and then reported the issue to Georgia Tech Cyber Security.

The Georgia Tech Cyber Security Operations Center (SOC) began investigating the vulnerability and identified that a malicious party exfiltrated data from the Student Information System (Banner) database.

Timeline

12/14/2018

A malicious party began utilizing a SQL injection vulnerability in the GT App to retrieve sensitive data from the Banner database.

3/21/2019

The EIS team enabled database audit logging in order to investigate a performance issue impacting financial aid application submissions. The database logs revealed an ongoing SQL injection attack impacting the GT App, which is used to support financial aid submissions, resulting in EIS developing a patch to remediate the SQL injection vulnerability.

3/22/2019

CHG0013205 (Appendix – Figure A) was approved to implement a patch to resolve the identified SQL Injection vulnerability. While Cyber Security has a representative on the Change Advisory Board, his approval was not requested for this change. This change was processed as an emergency change and approved by the Change Manager as part of the standard emergency change process.

3/26/2019

The EIS team sent an email to the SOC including information about the vulnerability and its remediation. The SOC opened a Security Incident (SIR0020348) in order to investigate the severity and impact.

3/27/2019

The SOC gained access to database audit logs and web server (IIS) logs for the affected application server (CFAPP02). By examining these logs, the SOC confirmed the SQL Injection vulnerability was successfully used by an external party to extract data by exploiting a web application and its underlying database (Banner). The SOC identified that the SQL Injection was conducted through URL parameters. See (Appendix – Figure B) for a sample database log.

3/28/2019
The SOC convened the Executive Incident Response Committee (EIRC). The EIRC distributed action items and agreed to begin initial notifications (Appendix – Figure C and Figure D) to the University System of Georgia (USG) and to the Department of Education (DoE). The SOC continued their analysis to determine the scope of exposure.

3/29/2019
The scope of the investigation broadened to include several other application servers related to the affected web application. The SOC conducted analysis on the IIS logs for the following systems to identify the tables and fields extracted by the outside party:

- CFAPPP01
- CFAPPP02
- CFAPPD01
- CFAPPD02
- CFAPPT01
- CFAPPT02

See (Appendix – Figure E) for a sample IIS log.

Due to the way the SQL Injection attack was performed, the SOC was able to verify the date, table and fields associated to each injection attack. The first date of data extraction was identified as 12/14/2018. See (Appendix - Figure F) for listing of tables and fields identified as part of the breach.

4/2/2019
The Institute Communications team disclosed the data breach to local media and an internal email communication (Appendix – Figure G) was sent by Information Technology to the Georgia Tech community.

The SOC coordinated with Institute Communications to publish a webpage (https://breach.gatech.edu) to communicate additional details to the public including Frequently Asked Questions (FAQ).

4/3/2019
The SOC filed a police report (Incident: 19040824) with the Georgia Tech Police Department (GTPD) and reported the data breach to the Federal Bureau of Investigation (FBI) Atlanta field office.

At the instruction of the EIRC, the SOC began gathering quotes from vendors capable of providing notification, credit monitoring, and call center services in the event the USG Cyber Insurance carrier would not cover this incident. In parallel, Georgia Tech Legal Affairs and the SOC worked with the USG to determine coverage by the insurance carrier.

The Legal Affairs team sent notifications (Appendix – Figure H) to consumer reporting agencies as required under the Georgia Personal Identity Protection Act of 2007, (O.C.G.A. 10-1-910, 10-1-911, and 10-1-912).

4/4/2019
The SOC provided additional incident details to the Department of Education's Office of Inspector General.

4/8/2019
The USG's insurance carrier retained the counsel of the law firm BakerHostetler. The SOC met with BakerHostetler to coordinate further recovery activities and direct the contracting of additional vendors.

BakerHostetler organized a meeting with Mandiant and Georgia Tech to discuss the investigation into the data breach and verify the findings of the SOC.

4/9/2019
The SOC provided Mandiant with log files, a high-level analysis report, and configuration details of the vulnerable system accessed by the outside party.

The SOC provided additional investigation details to the Federal Student Aid Cyber Incident Team (FSA).

BakerHostetler organized a meeting with Georgia Tech and Ankura Consulting Group, a data analysis firm, to discuss performing data analysis services in order to validate the individuals impacted by the breach.

4/10/2019
The SOC conducted a follow up call with Mandiant. The initial analysis conducted by Mandiant confirmed the tables and fields identified by the SOC's investigation.

4/12/2019
BakerHostetler sent a General Data Protection Regulation (GDPR) notification letter to the Commission nationale de l'informatique et des libertés in France.

The Georgia Tech Cyber Security investigation was closed by the SOC pending the findings of Mandiant.

Financial Impact
As a result of the incident, Georgia Tech filed a claim with USG's cyber insurance provider. The insurance provider facilitated the engagement of external vendors to provide appropriate incident response services. The fees for these vendors to be paid by the insurance provider are enumerated below:

Vendor	Cost
BakerHostetler	$77,140
IDExperts	$1,617,980
Ankura	$21,500
FireEye	$144,000
Total	**$1,860,620**

*A $10,000 deductible was incurred to file a claim with the insurance provider

In addition to the external services required, a large number of Institute employees were involved in response efforts. An estimate of hours and cost is outlined below:

Labor Type	Estimated Hours	Estimated Cost
Staff	820	$36,703.20
Executive	1075	$98,385.50
Total	**1895**	**$135,538.70**

*The estimated cost totals were calculated using an executive average labor cost of $90.14 per hour and a staff average labor cost of $44.76

Lessons Learned

Due to the scale and magnitude of this incident, Georgia Tech Cyber Security has departed from the standard "lessons learned" format for this section of the incident report. Normally, this section of the document would cover a list of items that could have prevented this specific incident, and we do cover these in the Technical Controls section, however, we have been asked many times how an incident such as this could have occurred despite the significant resources that the Institute has devoted to our Information Security program. In the following sections, we will try to explain how and why these incidents can still occur despite that investment.

Additionally, we have outlined the significant changes that need to be made to the business processes of the Institute to reduce the risk of an incident of this magnitude occurring in the future. It is important to note that though these changes require substantial work from Georgia Tech IT, they are fundamentally business process changes and how users treat data must change for IT to be able to succeed in these mitigations.

A common thread underlying these sections is a difference in understanding between the business owners and information technology of what the risks are and who has responsibility for performing the tasks necessary to mitigate the risk via business process or technical intervention. Over the past several years, when IT and business units have discussed that certain business processes are inherently risky, IT understood that the business unit was accepting the risk by not changing the process and the business unit understood that IT was able to monitor or allow the risk to remain. Both understandings have proven to be incorrect and create an environment where technology cannot prevent security risk because the underlying business processes are inherently risky.

IT and Data Governance, Risk, and Compliance

At present, the Institute has no formal body that accepts or manages risk, no formal structure for the approval of new IT systems or transfers of Institute data, and no formal process to evaluate compliance with IT policies. This is both created by and further enforces a culture where IT develops solutions to user problems prioritizing speed and cost of execution over long term support, information architecture, and risk.

As currently structured the Cyber Security department is responsible for assessing risk in multiple ways however there is not a defined group responsible for addressing IT Risk where Cyber Security may report identified issues. This creates several issues with how risks are reported and addressed:

- Today there may be risk to systems and data at the Institute that are not being effectively managed by business units outside of IT. For example, the need to retain 1.3 million records containing Social Security numbers is a risk that has historically

been raised by IT and Cyber Security. The potential need for these records has historically outweighed concerns about the impact of a breach involving these records. Ideally this sort of risk decision should be made by an official risk governance body that is supported by a team of people situated in an appropriate part of the organization that is charged with identifying, measuring, and reporting these risks.

- There is an inherent tension between IT's mission to deliver frictionless services and Cyber Security's mission to identify, measure, report, and mitigate IT risk. Despite the natural tension, it is vitally important for basic Cyber Security requirements to be prioritized so that risks are known and can be appropriately mitigated.
- Cyber Security is frequently asked to design IT services rather than advising on the risk of an existing or proposed service design. This is a conflict of interest as a person or group cannot effectively report risk on a service they designed.
- IT personnel are some of the most likely to pose an insider threat to data and there is a potential for conflict in Cyber Security investigating personnel within the same department.

Before this incident, the application group that developed the compromised application was approached by the Financial Aid department with a problem that our student information system could not solve. As requested by the customer, they created a solution to the problem that involved almost no direct cost in systems or personnel. However, this solution introduced risk that data would be inappropriately accessed. Currently, this type of risk is not catalogued, evaluated, or managed within Georgia Tech's administrative processes. Additionally, this type of risk is implicitly encouraged by our budgeting processes. Units frequently receive budget to develop a solution to a problem but are denied on-going budget to effectively support the solution.

This practice impacted this incident in several ways:

- First, this system was developed without formal analysis of risk. This allowed credentials and hosts to be reused. Additionally, at multiple points in the process of both developing and maintaining this system assumptions were made that data was protected somewhere else including at least that:
  - web app scanning would catch any security errors in the site design,
  - firewalls would prevent intrusion into the system,
  - encryption would prevent exfiltration of the data, and
  - the login page would limit exposure to campus users.

  None of these proved to be true because at each point there were gaps that could have been caught with another process but no wholistic process analyzed the risk of the overall system.
- Second, there were two prior incidents involving ERP systems where several recommendations were made including reducing the amount of data stored in and further restricting access to the system. However, several of these recommendations were never implemented nor was the risk formally accepted. The risks of not following these recommendations were presented to the business owners, but without a formal risk organization the true cost of this risk was not fully appreciated.
- Third, several internal policies were not followed on this system, most especially "Regularly review server logs looking for any inappropriate activity" (Data Protection Safeguards 8-5). Even if new policies are established following this incident, without regular or continuous audits Cyber Security cannot establish that they are followed.

- Finally, as a result of no group within the Institute having an overall picture of data management, GDPR requests following this incident resulted in a substantial undertaking as dozens of independent units were forced to catalog information they held on specific students.

Short Term Governance Recommendations

- Establish an IT Risk Management body including representatives from Ethics, Compliance, and Legal Affairs; Cyber Security; and Business Owners responsible for identifying and managing risk. This body should be empowered to determine if identified risks should be accepted, mitigated, or avoided. This could include denying projects where the risk cannot be sufficiently mitigated to offset the value of the project. This body's scope of authority should encompass the entire Institute.
- Establish an official path or process for Cyber Security to report IT risk directly to the official risk management body that is sufficient to mitigate the tension between IT service delivery and IT risk management.
- Revise Data Protection Safeguards to align with industry standards (e.g. NIST 800-171 and PCI DSS)
- Continue building log management platform and ingest all logs from high-risk systems including both server and application logs

Long Term / High Effort Governance Recommendations

- Develop processes to track all data transfers of student information and approve all new transfers to both new on campus systems and third-party systems
- Projects accepted by IT Governance should either be funded in full (including costs for long term support) or delayed until there is budget within the Institute to fully support the project including ongoing support and maintenance costs.
- Establish IT audit processes to evaluate the compliance with IT policy
  This process should be continuous to offer real-time validation so that non-compliance can be corrected.
- As part of implementing IT Service Management, fully document the process for turning an experiment or project into a production service.

Technical Controls

There were technical controls that could have been applied to these systems to dramatically reduce the likelihood and impact of this incident. **It is important to realize that though these controls may have prevented this incident, they are not the most important reason that a breach of this magnitude occurred.** While technical controls are extremely helpful in preventing and remediating security risks, the underlying business processes must be modified to reduce the reliance on technical controls, which on their own will never be able to prevent all incidents.

Short Term Technical Recommendations

- Implement a Web Application Firewall (WAF) in front of all applications exposing sensitive data to the internet
- Decrypt traffic to sensitive servers on existing layer-7 firewalls to allow better inspection of traffic
- Continue building log management platform and ingest all logs from high-risk systems
- For applications where access from the Internet is required, but the audience has GT accounts, implement a clientless VPN

Long Term / High Effort Technical Recommendations

- Implement User Behavior Analytics to identify abnormal access to applications and databases
  User Behavior Analytics products baseline the use of credentials and patterns of access in order to alert on deviations from the normal patterns. In this incident, since the vulnerable application (GT App) did not normally access the type and quantity of data that the adversary initiated, user behavior analytics software would have identified the access pattern as abnormal.

Data Minimization

There is an inherent and quantifiable risk for any organization to retain data about individuals. Georgia Tech must change to formally adopt the practice of limiting the collection of personally identifiable information (PII) including but not limited to social security numbers, student data, personal health data (PHI), and data regulated by the European Union General Data Protection Regulation (EU GDPR) to only that necessary for accomplishing the Institute's goals. **The useful and allowable life of the PII which Georgia Tech collects should be identified and the PII removed once that life is exceeded**. These practices should be formally documented in Institute policy and, at minimum, should comply with the USG policy (https://www.usg.edu/records_management/schedules/).

Currently Georgia Tech keeps, for perpetuity, nearly all information collected on individuals both affiliated and unaffiliated with the Institute and stores much of this data in a small number of massive databases. There are multiple systems making use of these databases, several of which are open to the entire Internet. Because of this design, a flaw in any of these systems allows the entire dataset, including data Georgia Tech no longer needs, to be retrieved by a malicious actor.

In this incident, many of the records breached were no longer required for the business needs of the Institute. Specifically, the current business process retains the Social Security Numbers of people no longer affiliated with the Institute. If those records had been expunged at the end of their useful life, it would have dramatically reduced the scope of data breached. If there is a need to keep infrequently used sensitive data, Georgia Tech should retain that data in a way that exposes it to the least amount of risk (e.g. archived offline).

Short Term Data Minimization Recommendations

- Define and implement retention policies for all sensitive data:
  Retention policies, including both minimum and maximum retention, should be established for all sensitive data elements. The USG records retention schedule should be the baseline for this Institute policy. Systems should be implemented to expunge records from central databases when the end of their useful life is reached and policies governing unit retention of data should specify that data should be purged when no longer needed.
- Expand the authority of an existing office or establish a new office responsible for data governance:
  The office would be responsible for the inventory and control of all of Georgia Tech's data. The office would establish processes and procedures for the collection, storage, and use of data and the compliance with all applicable regulations. The office would engage with business units to rethink or redesign business processes to align with retention policies. Georgia Tech, through this office, should change how data is

managed to be in line with industry best practices in Enterprise Data Management such as the DCAM Framework from EDMCouncil.

Long Term / High Effort Data Minimization Recommendations

- Establish a catalogue of locations where sensitive data is stored across the Institute and audit data retention:
  Establish a data map or catalog documenting where personal data collected on persons associated with the Institute are transferred and how long they are needed in each location. Policy should address that elements be purged from a location when their use is no longer supported by the reason specified in the catalog.
- Implement a Data Loss Prevention program:
  The data governance office would be tasked with creating a data loss prevention program. This would involve creating data classification tags, implementing methods of classifying data, and training users to classify the data they create. The data protection office would then work with Georgia Tech IT to implement controls to protect data relevant to its classification.

Least Privilege

Georgia Tech should adopt and enforce the concept of least privilege– that only the minimum amount of access is granted to a person or account that is needed to accomplish the duties and goals of the Institute. These privileges should be granted to roles instead of individuals and be provisioned and deprovisioned with the life cycle of the employee. **Individuals and applications should not have access to data they do not require** to support the goals and mission of the Institute. This model should follow the data categorization policies established at the Institute and allow for easy access to non-sensitive (public) information while enforcing stringent controls on sensitive information.

Currently, credential and scope reuse are extremely common in Georgia Tech information systems. As an example, if an account has been granted access to accomplish one task and another task comes up for which that level of access is sufficient it is common to reuse the account rather than evaluate what access is required for the new use case and generate a new credential. Because there is no central access management it is also common practice for applications to allow any valid account to access the system, even if that account requires no access at all. This is complicated by a preference to work with data sources in total rather than create restricted views where an application only gets access to part of the data stored in the data source.

The example above manifested itself in this incident. The compromised application required access to substantially less data than its permissions allowed. At most, it required access to the Social Security Numbers of current students, but it may have required substantially less than that. If the system only had access to those records required for its function it would have dramatically reduced the scope of data breached.

Short Term Least Privilege Recommendations

- Assess the current use of access credentials and issue new, more limited, credentials following the concept of least privilege:
  This includes database and application credentials for both people and service accounts. This may also require the creation of database views or other ways to restrict access to data more granularly than the table level.

Long Term / High Effort Least Privilege Recommendations

- Simplify the Identity and Access Management platform:
  Georgia Tech has an extremely complex identity management system, which is composed of custom written code, open source applications, and several off-the-shelf identity management products. Much of this complexity is born from the desire to satisfy the needs of custom business processes. Georgia Tech should re-evaluate its business processes in order to conform with the processes supported by commercial off-the-shelf products.
- Centralize access management to control access into critical applications:
  Georgia Tech lacks a system to centrally control access to information systems. While there exists a system to grant roles, it delegates access control implementation to the individual application owners. Delegating access in this manner causes at least three major issues: it leaves unnecessary room for error, precludes the ability to enumerate what an account or application can access, and prevents the audit of which accounts have access to particular data elements.

Information Architecture and Security/Privacy by Design

Information services provided at Georgia Tech should be offered through a consistent, well thought out enterprise architecture with data management, information security and privacy designed into the base architecture. Services should be offered by specialists who can assist in architecting a solution to meet the needs of the business including security requirements.

Currently Georgia Tech is structured so that most IT services are designed and supported by generalists at the business unit (i.e. school or lab) level. The central Georgia Tech IT department provides only high-level infrastructure support and delegates both authority and responsibility for service development to other IT units. This practice results in ineffective use of resources and inefficiencies of policy propagation and management.

At present, systems containing both public and sensitive data are distributed across many of these unit level IT environments, requiring security and privacy controls to be applied evenly across the entire enterprise in a less effective one-size-fits-all strategy. What often results is the least restrictive set of privacy and security controls are applied to both public and sensitive datasets.

Additionally, because much of the infrastructure has grown organically from small unit-driven projects into enterprise systems, **security, privacy, and scalability are often an expensive and ineffective bolt-on to the system rather than a design feature**. It is possible to further optimize security resource allocation while also saving the Institute money by incorporating security and privacy as a factor in data system architecture.

In this incident, the affected application was hosted on the same server/system as many other applications, some of which required public access. Because traffic to the host could only be restricted to the application which required the broadest access, the system was accessible to the entire Internet. Additionally, it is currently impossible to target advanced security features to high-risk systems because they are not isolated from low-risk systems.

Short Term Information Architecture Recommendations

- Inventory all public/Internet facing enterprise web applications and services:

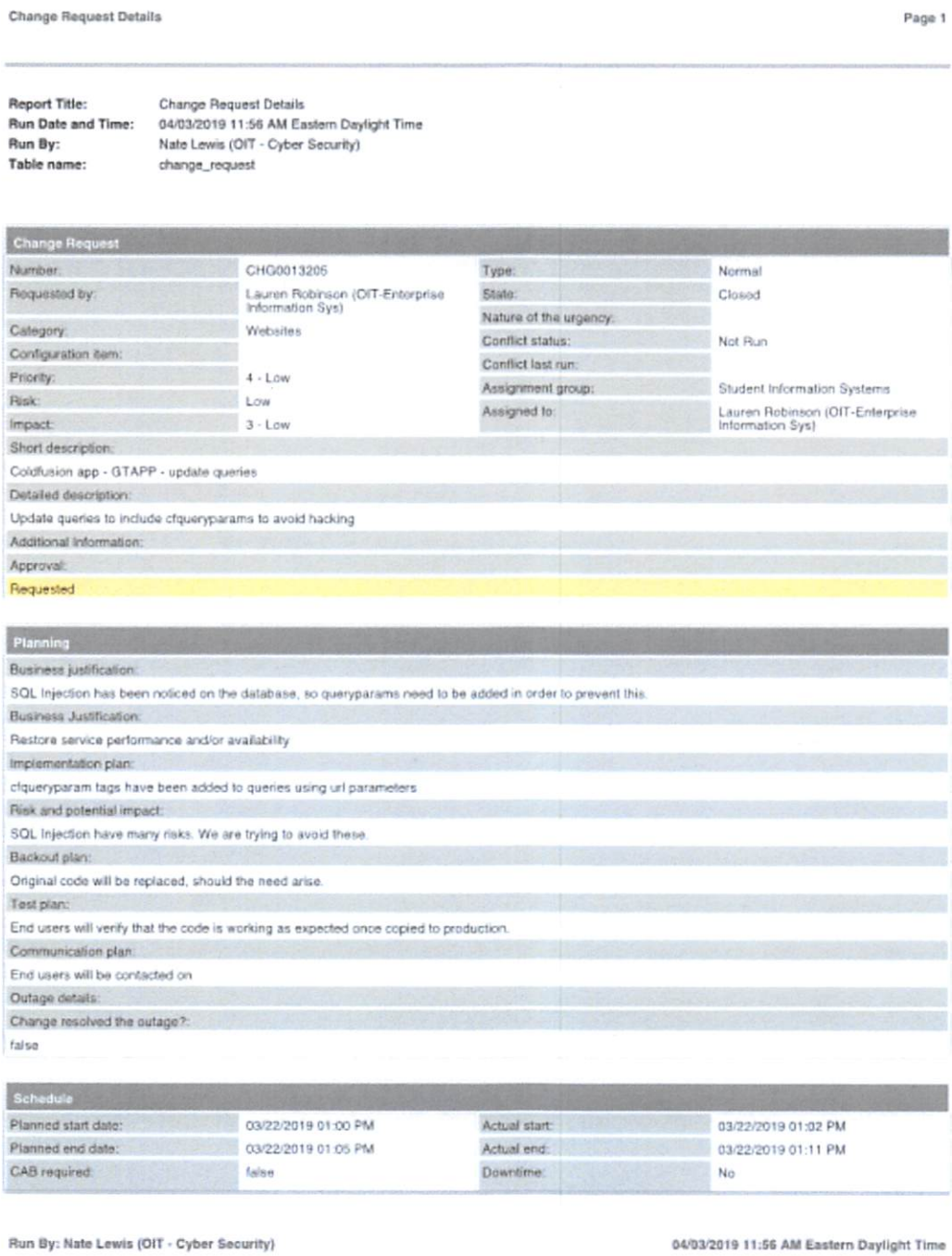
IT should continue efforts to populate a service catalog and a configuration database so that it can easily identify which enterprise applications should be exposed to the Internet and if any can be decommissioned or replaced.
    - Identify applications that are developed in-house or no longer supported by their manufacturer and categorize them as high risk
    - Identify if any of these applications are good candidates for replacing with commercial off-the-shelf software.
    - Identify audience for each application and restrict network access to minimum necessary scope
- Integrate a security code-review process into all new and existing in-house application development:
  Before an application is put into production, both programmatic and human analysis of the code should be performed to identify and remediate any security vulnerabilities present. Conduct code review on all existing applications. Remediation efforts should immediately take place for high-risk systems.
- Develop a security and privacy training program including secure application development training to all application developers and security training for IT administrators:
  Training should be provided to all Georgia Tech employees that develop code for applications covering common application security and privacy flaws and methods of producing proper code. Additionally, training should be offered to IT admins and service owners covering threat modeling and how to design security into information systems. Other training for those handling sensitive information should be identified and required for those granted access to this information.

Long Term / High Effort Information Architecture Recommendations

- Periodically review the architecture of all Georgia Tech applications:
  Much of Georgia Tech's information architecture is old and no longer adheres to current best practices. IT should review application architecture for all enterprise applications and make changes to bring them in line with external benchmarks such as the OWASP Top 10 or CIS 20 Critical Security Controls.
- Design and implement services using specialized service architects:
  IT services should be designed and fully owned by a service owner within Georgia Tech IT. Georgia Tech IT should transition from offering infrastructure to offering full IT services to prevent development by less qualified IT generalists. Service owners should also understand their ownership in driving governance within their service area including addressing issues such as adoption and compliance with standards.
- Include security and privacy in the design process in all new and revisited architecture projects:
  Georgia Tech IT should consider creating a department of IT architects responsible for the design of the Georgia Tech IT environment as a whole
- Establish high-risk data classification and align controls to other high-risk data control standards such as PCI DSS and NIST 800-171
- Design data center and campus networks to isolate systems storing or accessing high-risk data elements from other systems in order to minimize the effort to secure high-risk elements
- Implement additional security controls for systems that store or process high-risk data:
  These tools should include the ability to decrypt enterprise web application traffic for inspection by security tools and regular penetration testing.

Appendix

Figure A - Change Request (CHG0013205)



Change Request Details — Page 1

Report Title: Change Request Details
Run Date and Time: 04/03/2019 11:56 AM Eastern Daylight Time
Run By: Nate Lewis (OIT - Cyber Security)
Table name: change_request

Change Request

Number:	CHG0013205	Type:	Normal
Requested by:	Lauren Robinson (OIT-Enterprise Information Sys)	State:	Closed
		Nature of the urgency:	
Category:	Websites	Conflict status:	Not Run
Configuration item:		Conflict last run:	
Priority:	4 - Low	Assignment group:	Student Information Systems
Risk:	Low	Assigned to:	Lauren Robinson (OIT-Enterprise Information Sys)
Impact:	3 - Low		

Short description:
Coldfusion app - GTAPP - update queries
Detailed description:
Update queries to include cfqueryparams to avoid hacking
Additional information:
Approval:
Requested

Planning

Business justification:
SQL Injection has been noticed on the database, so queryparams need to be added in order to prevent this.
Business Justification:
Restore service performance and/or availability
Implementation plan:
cfqueryparam tags have been added to queries using url parameters
Risk and potential impact:
SQL Injection have many risks. We are trying to avoid these.
Backout plan:
Original code will be replaced, should the need arise.
Test plan:
End users will verify that the code is working as expected once copied to production.
Communication plan:
End users will be contacted on
Outage details:
Change resolved the outage?:
false

Schedule

Planned start date:	03/22/2019 01:00 PM	Actual start:	03/22/2019 01:02 PM
Planned end date:	03/22/2019 01:05 PM	Actual end:	03/22/2019 01:11 PM
CAB required:	false	Downtime:	No

Run By: Nate Lewis (OIT - Cyber Security) — 04/03/2019 11:56 AM Eastern Daylight Time

Figure B – Database Audit Log

```
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>>
Connection[138].setAutoCommit(boolean autoCommit)
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>> autoCommit = true
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>> OK
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>>
Connection[138].setTransactionIsolation(int level)
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>> level = 2
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>> OK
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>>
Connection[138].setReadOnly(boolean readOnly)
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>> readOnly = false
spy(ajp-nio-8016-exec-193)(2019/03/22 11:46:12.566)>> OK
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> Connection[138].isClosed()
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> OK (false)
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> Connection[138].getAutoCommit()
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> OK (true)
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> Connection[138].getMetaData()
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> OK (DatabaseMetaData[1681513])
spy(ajp-nio-8016-exec-232)(2019/03/22
11:46:12.566)>> DatabaseMetaData[1681513].supportsGetGeneratedKeys()
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> OK (true)
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> Connection[138].createStatement()
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> OK (Statement[1677880])
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>>
Statement[1677880].execute(String sql, int autoGeneratedKeys)
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> sql = select worgtam_title Title,
        worgtam_parm1 BegYear,
        worgtam_parm2 EndYear,
        worgtam_parm3 AidYear,
  worgtam_seq_no seqno
from worgtam
where worgtam_seq_no = ctxsys.drithsx.sn(1,(chr(33)||chr(126)||chr(33)||(SeLeCt CaSt(t as
char(255)) FrOm (SeLeCt rownum r, (SPRADDR_STAT_CODE) as
t FrOm SATURN.SPRADDR) WhErE r = 1997786)||chr(33)||chr(126)||chr(33)))
    and worgtam_option_url = 'verify_form.cfm'
    and SYSDATE between NVL(worgtam_start_date, SYSDATE)
     and NVL(worgtam_end_date, SYSDATE)
spy(ajp-nio-8016-exec-232)(2019/03/22 11:46:12.566)>> autoGeneratedKeys = 1
spy(ajp-nio-8016-exec-212)(2019/03/22 11:46:12.753)>> java.sql.SQLException:
[Macromedia][Oracle JDBC Driver][Oracle]ORA-20000: Oracle Text error:
DRG-11701: thesaurus !~!!~! does not exist
ORA-06512: at "CTXSYS.DRUE", line 160
ORA-06512: at "CTXSYS.DRITHSX", line 549
ORA-06512: at line 1
ErrorCode=20000 SQLState=HY000
java.sql.SQLException: [Macromedia][Oracle JDBC Driver][Oracle]ORA-20000: Oracle Text error:
DRG-11701: thesaurus !~!!~! does not exist
ORA-06512: at "CTXSYS.DRUE", line 160
ORA-06512: at "CTXSYS.DRITHSX", line 549
```

Figure C – University System of Georgia (USG) Notification

SENSITIVE SENSITIVE

University System of Georgia Cybersecurity Incident Report Form – Initial Report

Reporter:	Andrew Nyhan	Institution:	Georgia Tech
Institutional Incident ID:	SIR0020348	USG Incident Number:	USG- INC0197811

Description of Incident:

On March 21, 2019 the Enterprise Information Systems (EIS) team identified a performance issue related to the GT App used to collect financial application information. The team turned on database audit logging and discovered a SQL injection attack against the Banner database by an outside party.

On March 22, 2019 the EIS team implemented a change to resolve the SQL injection vulnerability.

On March 26, 2019 an email communication was sent to members of the Cyber Security team requesting security review of the GT App in order to identify any additional vulnerabilities. Cyber Security raised a Security Incident and began investigating the initial vulnerability and potential disclosure.

On March 27, 2019 the Cyber Security team gained access to audit logs from the EIS team. At approximately 10:30 PM EST the Cyber Security identified Personally Identifiable Information (PII) was queried by the outside party.

On March 28, 2019 the Cyber Security team convened the Executive Incident Response Committee (EIRC) to discuss notification and recovery.

What, if any, actions were taken at the time of and/or following discovery prior to contacting USG Helpdesk?

Actions Taken:
- Site was updated by application owner to re-mediate the exposed vulnerability
- Cyber Security is conducting forensic analysis to determine the scope of the data exposure
- EIRC was convened to initiate the notification process

Pending Action Items
- Office of Scholarships & Financial Aid
o Send communication to the Department of Education to comply with FERPA requirements

- Legal Affairs
o Notify USG Legal affairs about the incident
o Collaborate with necessary parties to draft and send the communication to the State of Georgia to comply with an exposure containing Social Security Numbers (SSNs)
o Perform analysis to determine if the event may warrant action as outlined under SOPP

- Cyber Security
o Notify USG Cyber Security about the incident
o Draft an incident memo to share with EIRC
o Share an incident notification template with EIRC

- Institute Communications
o Public
Draft media release
Prepare communication template to notify affected parties
o Internal
Prepare communications to affected users

- Executive Response Committee
o Determine if the event warrants the need to provide Identity Protection or Credit Monitoring Services
If yes, involve USG to understand if this will be covered under a Cyber Security Insurance Policy

Time and Date of Incident:	12/14/2018	Time and Date of Discovery:	3/26/2019
Did the incident involve PII:	Yes	Total or Estimated Number:	
Did the incident involve PHI:	No	Total or Estimated Number:	
Does the incident contain notice triggering information?		Yes	
Has/will the matter be reported to Law Enforcement?		No	
System Assigned Name:	CFAPPD01	System Assigned IP:	130.207.241.166
System OS:		System Location:	

Institutional Information Security Officer:	Institutional Alternative Contact for Incident:
Jimmy Lummis jimmy.lummis@security.gatech.edu 404-385-0334	Christopher Craig christopher.craig@security.gatech.edu 404-385-4316

V.1.1 – 10-2018

Please note that USG Cybersecurity or the Georgia Bureau of Investigations may contact the institution for additional information for further investigation.

SENSITIVE SENSITIVE

Figure D – Department of Education (DoE) Notification

Subject: FW: Unauthorized Data Disclosure

March 28, 2018
U.S. Department of Education,

In regard to the statement on your website related to an unauthorized disclosure or breach of applicant or other sensitive information (quoted at the end of this message), we wish to report the following:

Summary:
On March 21, 2019 the Georgia Tech Enterprise Information Systems (EIS) team identified a performance issue related to the GT App used to collect financial application information. The team turned on database audit logging and discovered a SQL injection attack against the Banner database by an outside party.

On March 22, 2019 the EIS team implemented a change to resolve the SQL injection vulnerability.

On March 26, 2019 an email communication was sent to members of the Georgia Tech Cyber Security team requesting security review of the GT App in order to identify any additional vulnerabilities. Cyber Security raised a Security Incident and began investigating the initial vulnerability that prompted the initial communication.

On March 27, 2019 the Cyber Security team gained access to audit logs from the EIS team. At approximately 10:30 PM EST the Cyber Security identified Personally Identifiable Information (PII) was queried by the outside party. This information includes but is not limited to:

- Social Security Numbers
- Driver's License Numbers
- Names
- Addresses

We are investigating the incident and will follow this notification with additional details as soon as we have them.
Source: https://ifap.ed.gov/dpcletters/attachments/20152016SAIGFormWatermarked.pdf
[The Destination Point Administrator]

DOE Statement
Must ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel. In the event of an unauthorized disclosure or breach of applicant information or other sensitive information (such as personally identifiable information), the DPA must immediately notify Federal Student Aid at CPSSAIG@ed.gov.

Figure E – Web Server [redacted] Log

u_ex190322.log:2019-03-22 15:46:12 130.207.160.162 GET /jakarta/isapi_redirect.dll - 443 - 3.95.147.116 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+pt-PT;+rv:1.9.1.2)+Gecko/20090729+Firefox/3.5.2+(.NET+CLR+3.5.30729) https://webapps.gatech.edu/cfeis/gtapp/verify_form.cfm?SeqNo=ctxsys.drithsx.sn(1%2c(chr(33)%7c%7cchr(126)%7c%7cchr(33)%7c%7c(SeLeCt+CaSt(t+as+char(255))+FrOm+(SeLeCt+rownum+r%2c+(SPRADDR_STAT_CODE)+as+t+FrOm+SATURN.SPRADDR)+WhErE+r+%3d+1997786)%7c%7cchr(33)%7c%7cchr(126)%7c%7cchr(33))) 200 0 0 1984

Figure F – Tables and Fields Accessed

[redacted]

Figure G – Internal Notification Email

Georgia Tech discovered that unauthorized access to a web application has exposed personal information for up to 1.3 million individuals, including current and former faculty, students, staff, and student applicants. The Institute's cybersecurity team is working to determine the extent of the access and to identify the affected individuals.

The information illegally accessed by an unknown outside entity was located on a central database. Georgia Tech's cybersecurity team is conducting a thorough forensic investigation to determine precisely what information was extracted from the system, which may include names, addresses, social security numbers, and birth dates.

Georgia Tech learned of the illegal access in late March and immediately took action to address the vulnerability. The Institute is committed to the privacy and security of its personal data and deeply regrets the potential impact on those affected.

The U.S. Department of Education and University System of Georgia (USG) have been notified. The Institute and USG hope to have more information soon, including how to determine who has been affected and next steps.

We continue to investigate the extent of the data exposure and will share more information as it becomes available. We apologize for the potential impact on the individuals affected and our larger community. We are reviewing our security practices and protocols and will make every effort to ensure that this does not happen again.

Figure H – Consumer Reporting Agency Notification

Good Afternoon,

On behalf of Georgia Institute of Technology ("Georgia Tech"), please see the attached notification letter regarding a data breach, pursuant to O.C.G.A. § 10-1-912(d).

Please contact Georgia Tech's Legal Affairs office if you have any questions regarding the notification letter.

Thank you.

Georgia Institute of Technology
Office of Legal Affairs

April 3, 2019

Sent via U.S. Mail only	*Sent via email only*	*Sent via email only*
TransUnion	Experion	Equifax
P.O. Box 2000	businessrecordsvictimassistance	securityinvestigations@
Chester, PA 19016	@experion.com	equifax.com

Recently, the Georgia Institute of Technology ("Georgia Tech") discovered that unauthorized access to a web application has exposed personal information for up to 1.3 million individuals, including current and former faculty, students, staff, and student applicants. This notice of the discovered breach is being provided to the nation-wide consumer reporting agencies pursuant to O.C.G.A. §10-1-912(d). The breach was discovered in late March 2019 and notice of the breach was sent to the Georgia Tech community (students, faculty and staff) on April 2, 2019 at approximately 8:50 am. The notice stated as follows:

+++notice begins
To the Georgia Tech campus community:

I want to inform you about an incident involving the exposure of personal data. Recently, Georgia Tech discovered that unauthorized access to a web application has exposed personal information for up to 1.3 million individuals, including current and former faculty, students, staff, and student applicants. The Institute's cybersecurity team is working to determine the extent of the access and to identify the affected individuals.

The information illegally accessed by an unknown outside entity was located on a central database. Georgia Tech's cybersecurity team is conducting a thorough forensic investigation to determine precisely what information was extracted from the system, which may include names, addresses, social security numbers, and birth dates.

Georgia Tech learned of the illegal access in late March and immediately took action to address the vulnerability. The Institute is committed to the privacy and security of its personal data and deeply regrets the potential impact on those affected.

The U.S. Department of Education and University System of Georgia (USG) have been notified. The Institute and USG hope to have more information soon, including how to determine who has been affected and next steps.

We continue to investigate the extent of the data exposure and will share more information as it becomes available. We apologize for the potential impact on the individuals affected and our larger community. We are reviewing our security practices and protocols and will make every effort to ensure that this does not happen again.

Sincerely,
Mark Hoeting
Vice President for Information Technology Chief Information Officer
+++notice ends

Additionally, notice was sent by Georgia Tech to the following media outlets on April 2, 2019 between 10:00 and 11:00 am:

- Atlanta Journal-Constitution
- Atlanta Business Chronicle
- WSB-TV
- WSB-Radio
- Fox5Atlanta (WAGA)
- 11Alive (WXIA)
- CBS46 (WGCL)
- Associated Press
- WABE-FM
- Georgia Public Broadcasting

That notice provided as follows:

+++notice begins
We are distributing the following information this morning:

--

Unauthorized Access on Georgia Tech Network Exposes Information for 1.3 Million Individuals

Unauthorized access to a Georgia Institute of Technology web application has exposed personal information for up to 1.3 million individuals, including some current and former faculty, students, staff and student applicants. Georgia Tech information security officials are working to determine the extent of the access and to identify the individuals who may be affected.

A central Georgia Tech database was accessed by an unknown outside entity. Georgia Tech's cybersecurity team is conducting a thorough forensic investigation to determine precisely what information was extracted from the system, which may include names, addresses, social security numbers and birth dates.

The U.S. Department of Education and University System of Georgia have been notified, and those whose data was exposed will be contacted as soon as possible regarding available credit monitoring services.

In late March, Georgia Tech learned of the illegal access and immediately corrected the impacted application. Georgia Tech is committed to the privacy and security of its personal data and deeply regrets the potential impact on those affected.
+++notice ends

Georgia Institute of Technology
Atlanta, Georgia 30332-0495 U.S.A.
PHONE 404.894.4812
FAX 404.894.3120