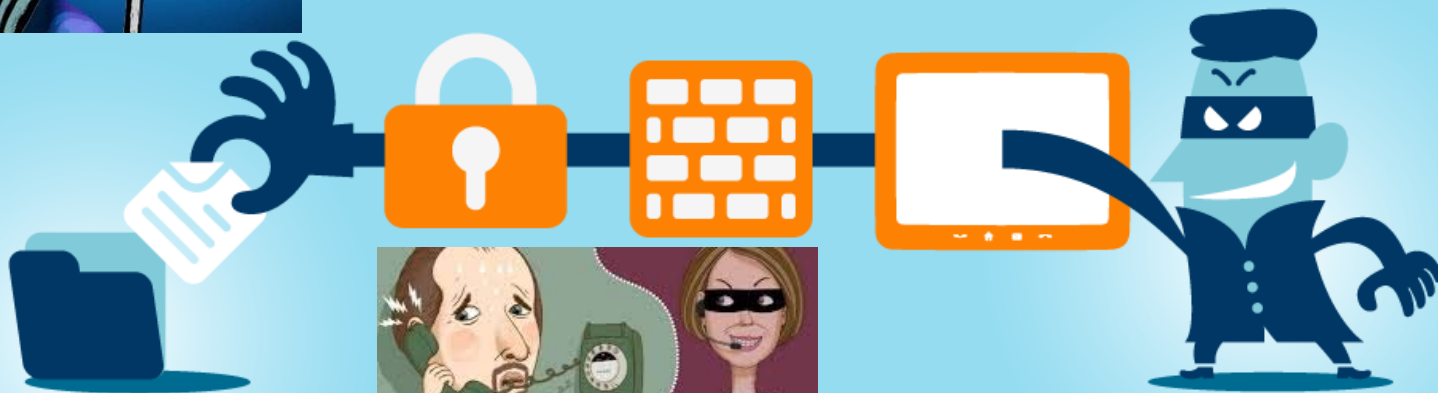


# County College of Morris Information Security Program

Really? I was not Aware

What do I need to Know?



Prepared by: John Young

# CCM's Information Security Environment

---

- External
  - Threats to the security of our data
  - Laws & Regulations (Compliance)
- Internal
  - Current assessment
- Next Steps
  - Where we need to be; and
  - Actions being implemented

# SECURITY BREACHES IN HIGHER EDUCATION



**35%**

of all security breaches  
take place in higher ed

SOURCE: <http://betanews.com/2014/12/17/35-percent-of-all-security-breaches-take-place-in-higher-education/>


## Most Common Types of Breaches in Higher Education

 **36%**  
Hacking


 **30%**  
Unintended Disclosure

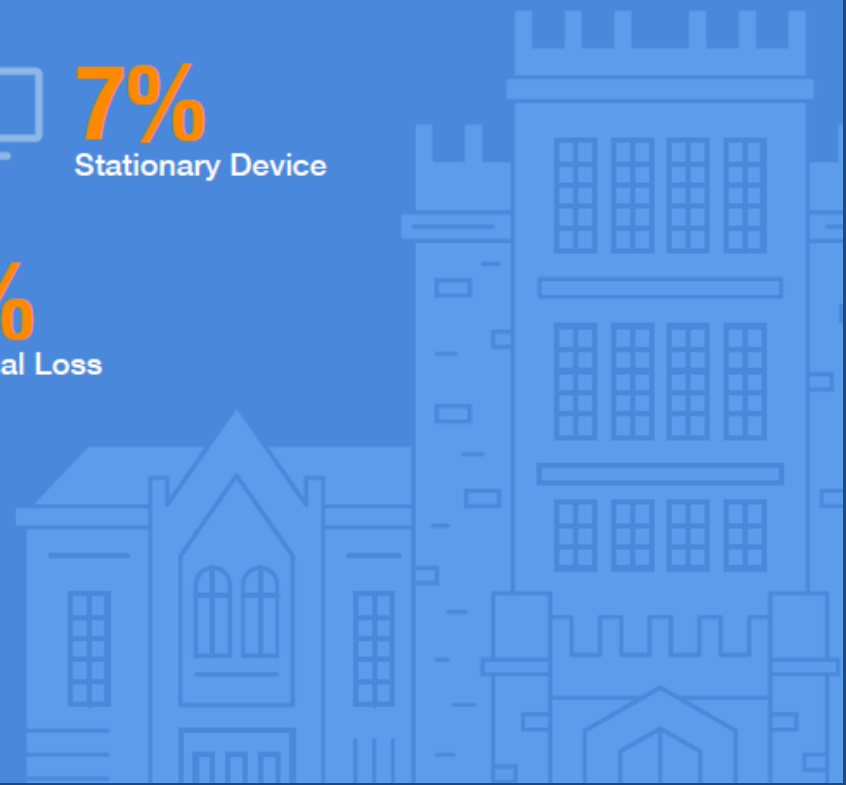
 **17%**  
Portable Device

 **7%**  
Stationary Device

 **5%**  
Physical Loss

 **3%**  
Insider

 **1%**  
Unknown/Other



<b>Date Made Public:</b>	January 10, 2018
<b>Company:</b>	Broward College
<b>Location:</b>	Fort Lauderdale, Florida
<b>Type of breach:</b>	<u>HACK</u>
<b>Type of organization:</b>	EDU
<b>Records Breached:</b>	44,000

On or about August 3, 2017, Broward College employees received a spam phishing email to their email accounts. The school learned that certain employees had clicked on the link and provided their credentials. Between July 18, 2017 and September 8 2017, Broward college determined that records were exposed including name, date of birth, address, social security number, financial account numbers, credit/debit card numbers, and/or driver's license or state identification card number. The breach affected 44,000 records.

*Information Source: Security Breach Letter*

<b>Date Made Public:</b>	June 16, 2014
<b>Company:</b>	Riverside Community College
<b>Location:</b>	Riverside, California
<b>Type of breach:</b>	<u>DISC</u>
<b>Type of organization:</b>	EDU
<b>Records Breached:</b>	35,212

Riverside Community College has suffered a data breach affecting 35,212 students. On May 30th, a district employee emailed a file containing information about all students who were enrolled in the spring term to a colleague working at home due to illness, for a research report that was on a deadline. The district employee used a personal email account to send the data because the file was too large for the district's secure email to send. The employee then typed in the incorrect email address.

The information contained in the file included names, addresses, birth dates, Social Security numbers, email addresses, student ID numbers, and telephone numbers.

<b>Date Made Public:</b>	January 5, 2016
<b>Company:</b>	Southern New Hampshire University
<b>Location:</b>	Hooksett, New Hampshire
<b>Type of breach:</b>	<u>DISC</u>
<b>Type of organization:</b>	EDU
<b>Records Breached:</b>	140,000

Southern New Hampshire University is investigating disclosure of a database that contained student information, The database contained more than 140,000 records including student names, email addresses, and ID's, course name, course selection, assignment details and assignment score, instructor names and email addresses.

The University claims that a third party vendor exposed the data due to a configuration error.

**More information:** <http://www.csoonline.com/article/3019278/security/snhu-still-investigati...>

*Information Source: Media*

<b>Date Made Public:</b>	July 22, 2017
<b>Company:</b>	Washington State University
<b>Location:</b>	Olympia, Washington
<b>Type of breach:</b>	<u>PHYS</u>
<b>Type of organization:</b>	EDU
<b>Records Breached:</b>	1,000,000

"When thieves broke into an Olympia storage locker in April and hauled away an 85-pound locked safe, they set in motion a series of events that forced Washington State University to send letters to 1 million people advising them their data might have been compromised.

The safe contained a computer hard drive — a backup containing personal information, including Social Security numbers, that was stored off-site by WSU's Social & Economic Sciences Research Center. The center, a research arm of the university, contracts with state agencies to evaluate the quality of the data those agencies are collecting, said Phil Weiler, vice president for marketing and communication at WSU.



<b>Date Made Public:</b>	July 23, 2010
<b>Company:</b>	University of California San Francisco (UCSF) Medical Center
<b>Location:</b>	San Francisco, California
<b>Type of breach:</b>	<u>INSID</u>
<b>Type of organization:</b>	EDU
<b>Records Breached:</b>	0

A former employee used the Social Security numbers of his colleagues to obtain vouchers for Amazon.com purchases. He secretly used the Social Security numbers to create hundreds of accounts and complete 382 online StayWell health surveys in exchange for \$100 online vouchers.

**UPDATE (10/28/10):** The former employee pled guilty to wire fraud and improper use of Social Security numbers. He was sentenced to 12 one year and one day in prison.

*Information Source: Databreaches.net*

# Compliance Landscape



# General Institutional Requirements

---

- FERPA, HIPAA, GLBA, RFR, and PCI-DSS share many of the same requirements:
  - Designate individual responsibilities
  - Risk assessment
  - Data security policies and procedures
  - Incident handling
  - Training and awareness
  - Compliance monitoring and adjustment

# Consequences of Noncompliance

---

- Loss of federal grant funding
- Loss of federal student financial aid
- Monetary penalties
- Lose ability to accept credit card payments

Also.....

Loss of reputation

Jeopardize accreditation

# Where We Need To Be / Steps To Be Taken

---

## Goals of the Information Security Program

1. Ensure security and confidentiality
2. Protect against anticipated threats (security and integrity)
3. Protect against unauthorized access/use

## Elements of the Program and Actions being Taken

1. Board Formally adopt CCM's Information Security Program.
2. Designate an Information Security Program Coordinator
3. Employee awareness and training
4. Identify and assess risks
5. Design and routinely test/monitor safeguards
6. Oversight of service providers
7. Evaluation and adjust (Assessment)

# INFORMATION SECURITY / USE OF TECHNOLOGY RESOURCE CENTER

(Located on the Faculty/Staff Page of CCM Intranet)

## College Policies

- Use of Information Technology (Policy # 2.20009)
- Identity Theft Prevention Program (Policy # 2.2014)
- Data Security (Policy # 2.2016)
- Information Security Program (In draft form; not posted)

## Other Policies

- FERPA – Family Educational Rights and Privacy Act

## Procedures:

### FERPA for Faculty and Staff

#### Procedure if a Breach of Personal Information Occurs:

- Personal Information Security Breach Notification Procedure
- Identity Theft/Breach of Personal Information Reporting Form

## Training Resources

- Identity Theft Prevention Training Module (Preventing, Detecting, and Mitigating Identity Theft)
- Measures for Identity Theft Prevention Reference Guide.
- Sensitive Data Protection Best Practices
- CCM's Information Security Program Update – Summer 2018
- Identity Theft Quiz



## Additional Resources

- Red Flags Rule (RFR)
- Gramm-Leach-Bliley Act (GLBA)
- New Jersey Identity Theft Act
- SANS Security Awareness Newsletter (Ouch!)
- Identity Theft Resource Center Website: Identity theft victim assistance, consumer information & data breaches.
- OnGuardOnline.gov: Federal government's website to help you be safe, secure and responsible online.

## Upcoming Additions to the Resource Page:

- Board Policy implementing CCM's "Information Security Program"
- HIPAA
- PCI-DSS
  
- Procedure Development Resources
  - Templates
  - Examples
  
- Reference Guides / How to / FAQ

# What Can I do? What is my Responsibility?

- Be aware and knowledgeable of information security and use of technology guidelines, policies, and procedures
- Safely manage our passwords
- Safely manage our email account
- Secure our computer and other college assets
- Protect the data we are handling
- Avoid risky behavior online

# Department Head Requirements

All departments/offices are required develop, maintain, and train employees on procedures and processes to protect personal information specific to their areas of responsibility.

*“Maintain documented procedures and processes that are understood and practiced by your employees”*

# REVIEW Your Current Procedures/ Processes

- Secure documents that contain identifying or protected data/information.
- Limit access to sensitive data/information.
- Avoid the use of social security number as an identifier and limit access to Social Security numbers.
- Collect only information that is necessary for your business purpose.
- Ensure complete and secure destruction of documents, computer files, and storage devices containing sensitive information.
- Ensure systems and computers are password protected and virus and vulnerability threat protections are up-to-date.

# REVIEW Your Current Procedures/ Practices

(continued)

- Sensitive data is not to be distributed via email or stored on external drives (USB, Thumb, Flash, etc.).
- Sensitive data stored on portable computing devices and storage media must be encrypted.
- Personally owned drives and devices are never to be used to store sensitive institutional data.
- Contractors and service providers are required to have safeguards in place to protect our sensitive data.

# *Questions*

# *Comments*

