




---

---

---

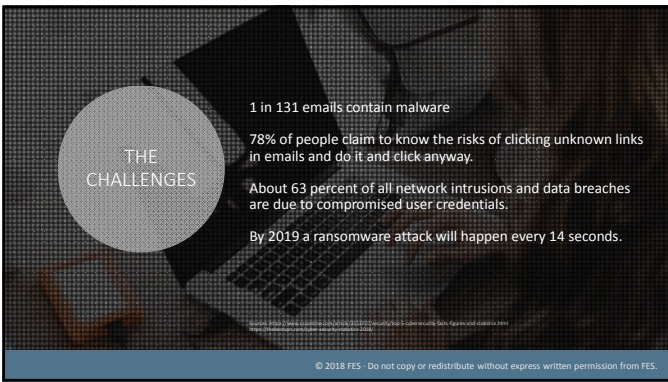
---

---

---

---

---




---

---

---

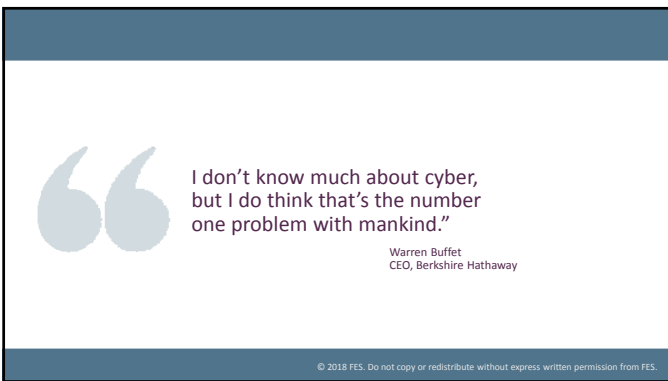
---

---

---

---

---




---

---

---

---

---

---

---

---

### A Day in the Life in the FAO

- Telephone calls from parents
- Specific information requested via email
- Student requesting to speak with a financial aid counselor with a friend or non-custodial parent
- Request from a FBI agent
- Request for ISIR data from another department on campus
- Receipt of PII via email and fax

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Protecting Your Students' Data

- Why Target a School?
- Top Five Data Security Issues
- ED Guidance and Recent Security Training
- Best Practices
- Security Tools and Resources
- Questions

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---


---

---

---

### Schools are a Valuable and Can be an Easy Target

- Stores a vast amount of long-term data
- IT challenges
  - Large number of records
  - International connections
  - Student access to internal resources
- New technology



© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Top 5 Data Security Practices

- Security Awareness
- Managing Passwords
- Forensic Logging
- Breach Response
- Third-Party Review

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Security Awareness

- Combination of knowledge and attitude
- Applies to everyone
- There is no such thing as common sense without a base common knowledge
- Security programs fail, because they assume there is the common knowledge

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Attack Methods That Exploit Uninformed Users

- Social Engineering
- Phishing
- Pharming
- Vishing
- Smishing

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---


---

---

---

### Multi-Tiered Approach to Delivery

- Presentations
- Posters
- Topical articles / current events
- On-the-job and role-based training



© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Password Management Characteristics

- Length
- Complexity
- Age
- Non-dictionary (any dictionary)

3Yx3FnmQVt%e2

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Passphrases

- Easier to remember
- Satisfies complex rules easily
- Major OS and applications supports passphrase
- Passphrases are next to impossible to crack

Passphrasesare#easier2remember

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

Forensic Accounting

If it wasn't written down,  
it didn't happen...

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

Forensic Accounting

When sensitive information is accessed, either physically or electronically, you should be able to positively identify:

- Who – individual person or user id
- What – information accessed
- Where the event occurred, or what systems the information was accessed on and from
- When – always time stamps and synchronized on your systems

Do not log actual PII, sensitive data, passwords, account information, etc.

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

Protection of Log Information

- Separate from systems that generate the logs
- Segregation of duties
- Logging failure notification
- Log reduction
- Tamper evidence

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Data Breaches

- Disqus – data breach from 2012 with info dating back to 2007
- Yahoo (update) – update from 1B impacted users to 3B
- Hyatt Hotels – unauthorized access to payment info, 41 properties, 11 countries
- Forever 21 – Point-of-sale devices compromised, unsure of reach
- Maine Foster Care– exposed PII, unsure of reach or use
- Uber – 57M users and drivers emails and phone numbers
- Imgur – 1.7M user codes and passwords
- TIO Networks – 1.6M customers, bank accounts, SSNs, payment info
- eBay - usernames, last names and purchase history of sensitive products
- Alteryx – 120M American households personal info

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Breach Response

Security professionals, to be successful, have to defend billions upon billions of attacks occurring 24 hours per day, 7 days per week, 365 days per year.

Successful attackers only need to be right **once**.

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Breach Response Incident Plan

- Technology owners, Business Process owners, Executive Management, Human Resources, Legal Counsel, and Communications
- Notifications to Data Owners, Local, State, and Federal government, Media relations, Law Enforcement

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Data Handling Compliance

- **NIST SP 800-53** – required by FISMA
- **NIST SP 800-171** – required for all secondary ed financial aid offices
- **Gramm-Leach Bliley Act** – record keeping for financial process
- **FERPA** - non-PII education records
- **PCI** – payment card info
- **HIPAA** – health info

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Third-Party Review

- Required by most controls
- Provides independent accounting of the Security Program
- Accountability to Senior Management

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### A Consistently Hot Topic



- ED Guidance Publications
- ED Webinar – *Post Secondary Institution Data Security Requirements and FSA Data Privacy/Sharing*
- NASFAA Webinar – *Best Practices in Applicant Data and Authentication Policies and Procedures*
- FSA and Professional Association Conference Sessions
- Recent Breaches

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

**Security Tools & Resources**

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

**Security Policies and Procedures Poll**

- Do you have written data security policies and procedures?
- Do you follow your written data security documentation consistently in your office?
- Do you have a written authentication protocol?
- Are data security practices consistent across campus?

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

**Best Practices in the School**

- Establish and consistently follow written policies and procedures on:
  - Authentication requirements for in-person, email and telephone inquiries
  - Management of both paper and electronic documentation
- Training and periodic reminders
- Include in employee performance program

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---



### Protecting Student Data is Priority

- Building with secured floors and cameras
- Badge policy
- Employee background checks
- Forensic audit trail
- Laptop security and clean desk policy
- Data security training and test requirements
- FISMA ready
- TECH LOCK Certified: Service Provider

FES protects the confidentiality, integrity and availability of student data.

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### FISMA Ready Importance

- NIST SP 800-53 rev. 4 defines the controls necessary for Federal Information Security Management Act (FISMA) compliance
- FISMA ready is the highest classification possible without having a federal contract

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### FISMA Ready Importance

What does this mean for schools?

These controls are the comprehensive management, operational, and technical safeguards (or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Security Laws and Guidelines

- NIST SP 800-53 r4 - <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- NIST SP 800-171 - <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf>
- GLBA - <https://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf>
- FERPA - <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- PCI-DSS - [https://www.pcisecuritystandards.org/document\\_library?category=pcidss&document=pci\\_dss](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss)
- HIPAA - <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Security Resources

- [\\$668.46 Institutional security policies and crime statistics](#)
- [Electronic Announcement 9/5/2017](#)
- [GEN 15-18](#)
- [GEN 16-12](#)
- [Protecting Student Privacy](#)
- [Federal Trade Commission Security Videos](#)
- [FSA Assessments](#)

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

### Summary

- Recommend an inclusive security awareness program
- Ensure passwords are long and complex, but memorable
- Record and protect activity logging
- Create a breach plan
- Require recent audits, compliance certifications and security standards from your current or potential third-party servicer

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

---

Questions

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---

Art Provost

ArtP@fes.org  
800.850.8397 | 402.479.6848  
www.fes.org

© 2018 FES. Do not copy or redistribute without express written permission from FES.

---

---

---

---

---

---

---