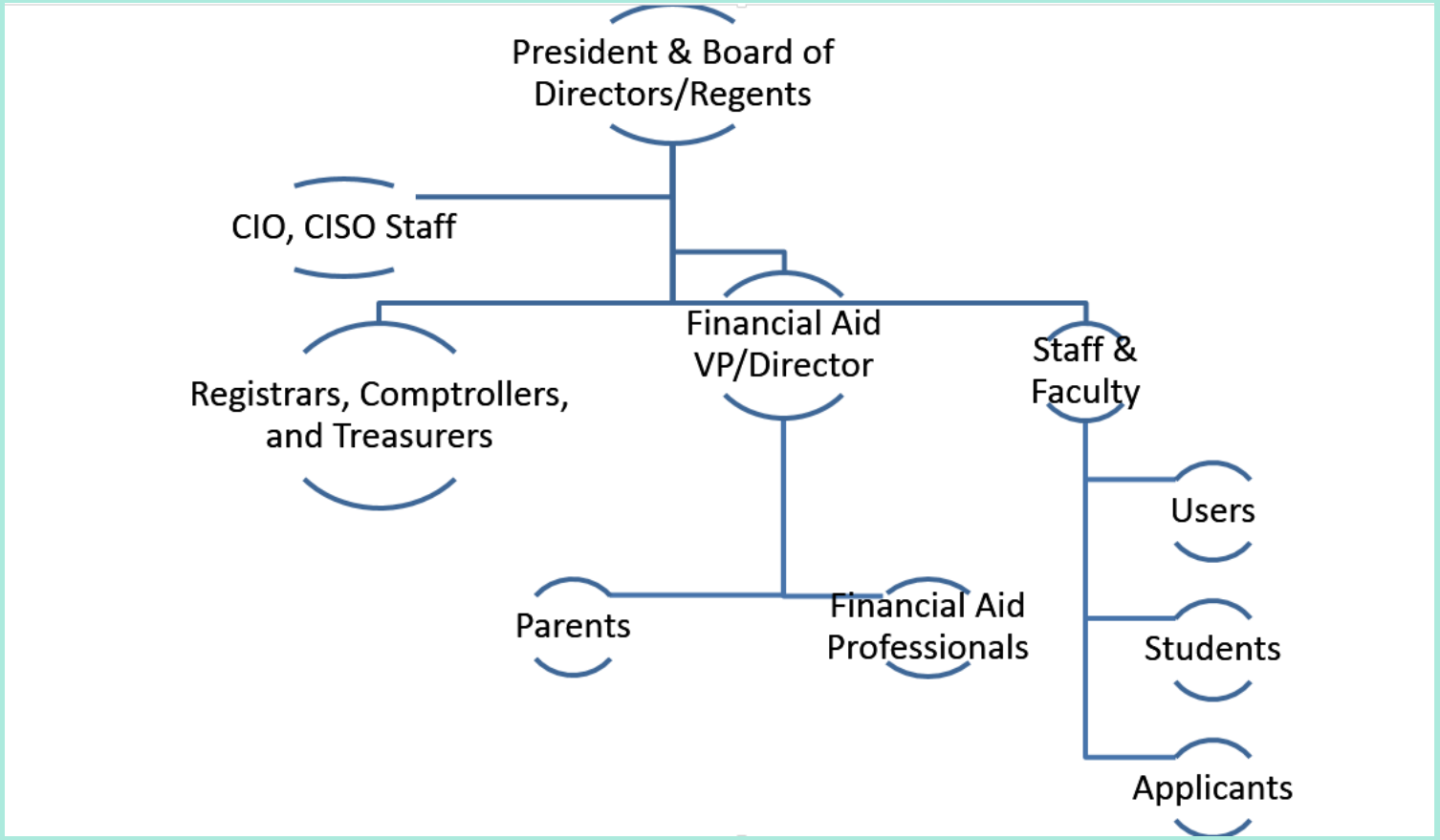
CYBERSECURITY: GLBA

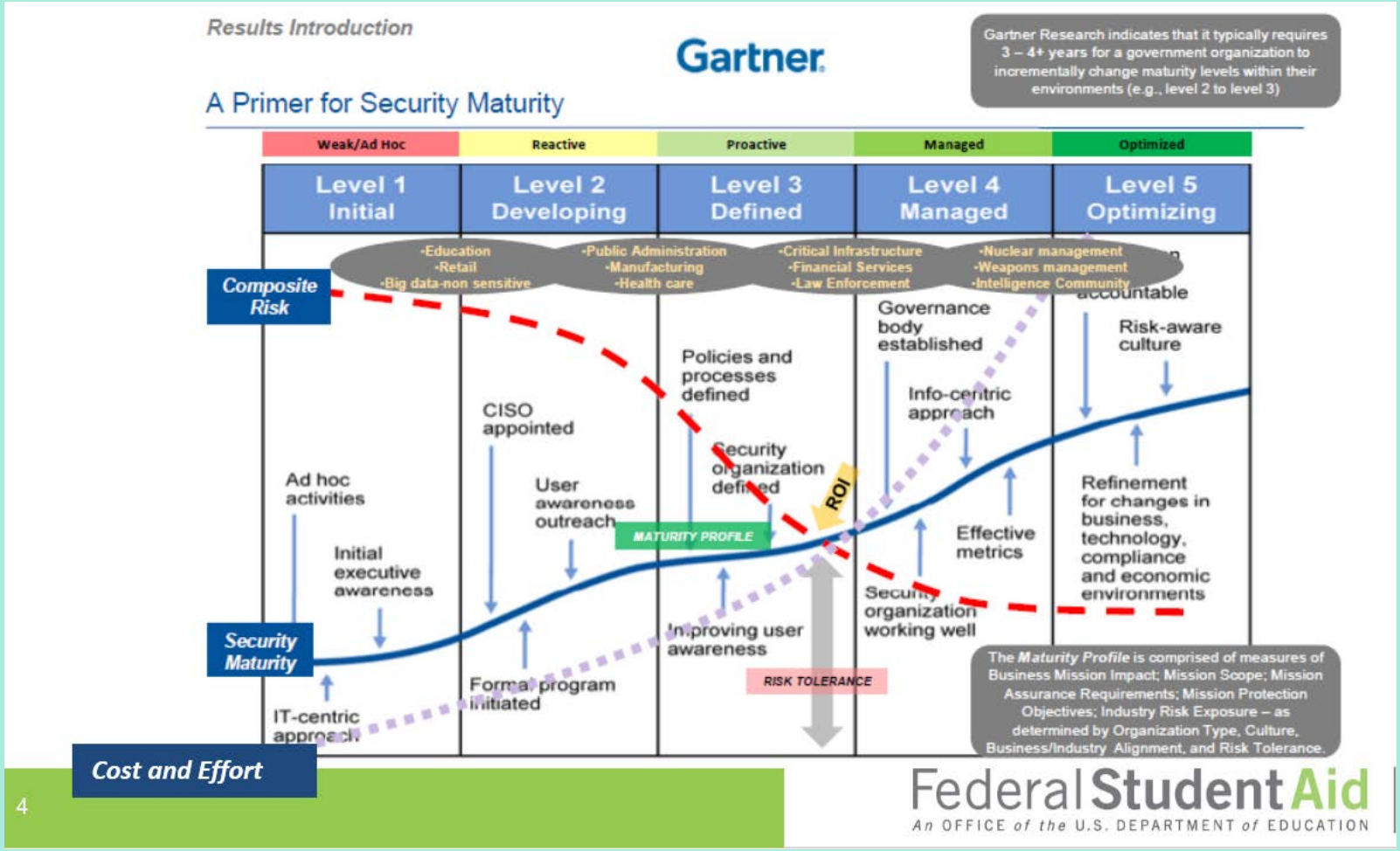
Presented by: Myrna Perkins, Chief Accreditation Officer | Director of Financial Aid

13-Feb-18

Who needs to worry about data security?



Educational institutions are specifically being targeted because of the current state of ad-hoc security coupled with the educational environment being a rich trove of emails, information, and research.



What protocols must post-secondary institutions follow to safeguard data?

- Family Educational Rights & Privacy Act (FERPA)
- Health Insurance Portability & Accountability Act (HIPAA)
- Federal Trade Commission – Red Flag Rule
- General Data Protection Regulation (GDPR)
- Gramm-Leach-Bliley Act (GLBA)

General GLBA Information

GLBA was enacted by Congress in 1999 to reform the banking industry. Colleges and universities are also subject to some of the provisions of GLBA because of the collection and maintenance of financial information of students and interactions with others. This requirement falls under the institution's Program Participation Agreement (PPA) with the U.S. Department of Education. Within the last two years there has been a heightened alert to protection of personal information. Higher education has become a prime target of hackers due to the vulnerability of students.

- July 29, 2015 – Dear Colleague letter was sent by ED alerting schools of the GLBA requirements.
- July 1, 2016 – Dear Colleague letter was sent by Ed alerting schools of the GLBA requirements.
- November 27, 2017 – The Government Accountability Office (GAO) issued a report stating an audit of ED's FSA procedures found several weaknesses in procedures for protecting student records.
- February, 2018 – The most recent audit guide will be released with newly added questions regarding cybersecurity.

Sanctions

- Title IV aid will be immediately revoked in case of a security breach. Depending upon the severity, institutions may indefinitely lose eligibility to participate in T4.

- $54,789 institutional fine per incident of non-compliance with GLBA.

- $10,000 personal fine – President, Chief Financial Officer, Director of Financial Aid

- ED's latest audit guide has questions regarding the institution's compliance with GLBA. If found unmet, the institution may face penalties.

Requirements – U.S. Department of Education

- Develop, implement, and maintain a written information security program;
- Designate the employee(s) responsible for coordinating the information security program;
- Identify and assess risks to customer information;
- Design and implement an information safeguards program;
- Select appropriate service providers that are capable of maintaining appropriate safeguards; and,
- Periodically evaluate and update their security program.

References

- https://ifap.ed.gov/eannouncements/Cyber.html
- https://ifap.ed.gov/dpcletters/GEN1518.html
- https://ifap.ed.gov/dpcletters/GEN1612.html
- http://www.uakron.edu/ogc/legal-policies-and-procedures/privacy-practices-and-policies/gramm-leach-bliley-act-glba.dot
- http://technology.pitt.edu/security/gramm-leach-bliley-act
- https://www.safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/glba
- http://www.nacubo.org/Search_Results_Page.html?q=glba
- http://www.webcastregister.live/2017fsatc_records/viewv2/294/
- http://www.webcastregister.live/2017fsatc_records/viewv2/287/
- https://www.gao.gov/products/GAO-18-121