Securing Federal Financial Aid Data with NIST SP 800-171

W. Jackson Schultz, CISA
Senior Consultant – IT Audit & Security
OCD Tech
jschultz@ocd-tech.com
www.ocd-tech.com

O'Connor & Drew P.C.
Certified Public Accountants

OCDTECH

Who We Are

- ✓OCD Tech is the IT Audit & Security arm of O'Connor & Drew, P.C.
- ✓O'Connor & Drew, P.C. was established in 1949 (67 year-old Firm).
- ✓We work with approximately 40 Institutions, both public and private, in various capacities.
- ✓Additionally, we audit a number of institution-related entities, such as various foundations of public institutions, the New England Board of Higher Education (NEBHE), New England Association of Schools and Colleges (NEASC), and the Association of Independent Colleges and Universities in Massachusetts (AICUM).
- ✓OCD Tech's team members are technicians first and auditors second, meaning we have an in-depth understanding of what requirements are asking for, and ***WHY*** they are in place.

IT Security in Higher Education

✓IT Security can be a challenge for higher education institutions due to ***lack-of-resources*** (both staffing and financial) and, in some cases, a ***mis-investment*** in technology and security.

✓Networks managed by colleges and universities have to remain ***open*** to students, facility, and parents.

✓The challenge is finding the happy medium of openness needed for respective parties and security controls to prevent ***malware*** and ***sensitive data exfiltration***.

Requirements and Guidance for Massachusetts Colleges and Universities

- ✓Health Insurance Portability and Accountability Act – HIPAA; 1996
  - ✓Universities, in some cases, are covered entities under HIPAA (and Privacy Rule).
- ✓Gramm-Leach-Bliley Act – GLBA; 1999
  - ✓Colleges and universities are subject to some of the requirements of GLBA because they collect and maintain financial information about students and others.
- ✓Federal Information Security Management Act – FISMA; 2002
  - ✓FISMA applies to federal contractors and organizations which maintain information on behalf of the government.
- ✓Massachusetts Privacy Law – 201 CMR 17.00; 2010
  - ✓Regulation passed to protect personal information (PI) of residents of the Commonwealth.
- ✓Dear Colleague Letter – GEN-15-18; 2015
  - ✓Letter reminding higher education entities about the protection of data used surrounding the administration of Title IV Federal student financial aid programs.
- ✓Dear Colleague Letter – GEN-16-12; 2016
  - ✓Letter reminding higher education entities of their legal obligations to protect student information used in the administration of the Title IV Federal student financial aid programs, as well as the methods the Department will use to assess institutions' capabilities in securing that information.

Threats to Higher Education

- ✓Cloud Security
- ✓Data Exfiltration
- ✓Data Security Specific Governance
- ✓Distributed Denial of Service
- ✓Environmental Disasters
- ✓Identity and Access Management
- ✓Malware
- ✓Personal Devices and Bring-Your-Own-Device
- ✓Phishing
- ✓Strategic Planning

Recent Events

February 8, 2016

63,000 Affected.

February 29, 2016

80,000 Affected.

March 28, 2016

Tax Season Scam

Recent Events

- ✓As a firm, we've developed a technology based on an industry standard to scrape the internet for usernames and passwords.

- ✓ Many of the usernames and passwords uploaded to sites commonly visited by hackers are login information for university systems.

- ✓In other words, generally, the emails uploaded by hackers and identified by OCD Tech are *@*.edu.

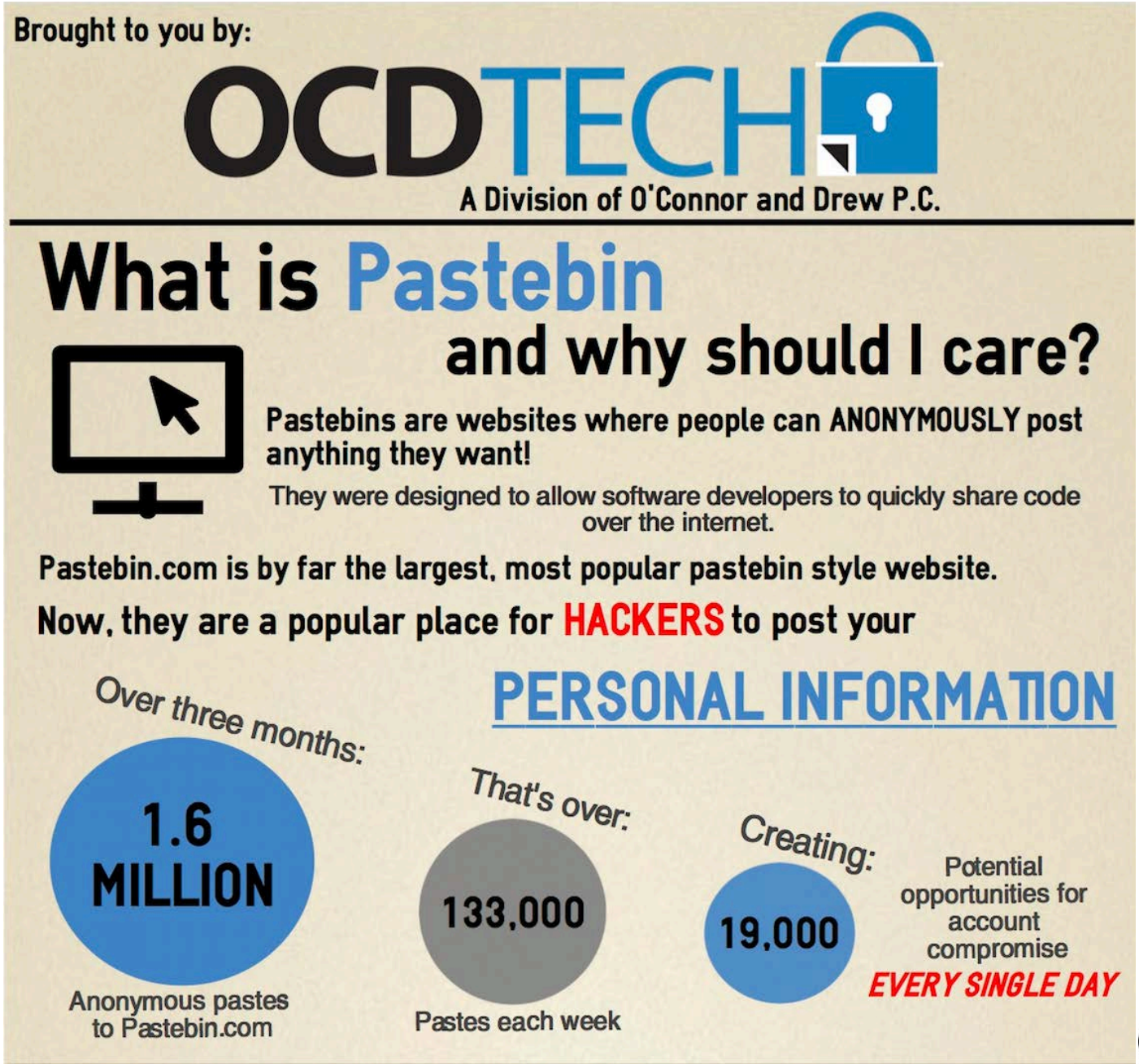
Recent Events

✓We reviewed our Pastebin data and sampled 9 colleges and universities who are members of AICUM.

✓We received 104 unique alerts about uploaded email addresses from each school.

✓Each alert contains a number of email addresses.

✓This does not necessarily mean that an institution has been hacked; this could be because of a third-party breach.


Brought to you by:
OCDTECH
A Division of O'Connor and Drew P.C.
What is Pastebin
and why should I care?
Pastebins are websites where people can ANONYMOUSLY post anything they want!
They were designed to allow software developers to quickly share code over the internet.
Pastebin.com is by far the largest, most popular pastebin style website.
Now, they are a popular place for HACKERS to post your
PERSONAL INFORMATION
Over three months:
1.6 MILLION
Anonymous pastes to Pastebin.com
That's over:
133,000
Pastes each week
Creating:
19,000
Potential opportunities for account compromise
EVERY SINGLE DAY

Sensitive Pastes By Data Type

Email and Password Dumps

3,459

Potential Credit Card Information

3,375

Pastes containing two or more IP addresses

102,064

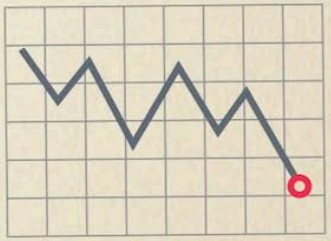
Every 45 minutes, a hacked email and password combination is posted to Pastebin.com

1. In 2015, the average cost of a lost or stolen record containing sensitive information was $154

2. The average data dump posted to Pastebin.com contains well over 100 records...

Source: https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

Everyday, stolen credentials posted to Pastebin.com can generate THOUSANDS of dollars in damages...



Wondering if your private information ...is still private?

For More Information:

Contact the Information Security Experts at OCD Tech

OCDTECH

OCDTECH

Areas for Improvement

- ✓According to an assessment performed by SANS Institute, published June, 2014 (sponsored by AlienVault, Tenable Network Security and Trend Micro), the areas needing enhancement within higher education are:
  - ✓Risk assessment
  - ✓Sensitive systems
  - ✓Sensitive data
  - ✓Lack of encryption
  - ✓Unclassified and unmanaged data
  - ✓Staffing and budgeting

Areas for Improvement

- ✓Risk Assessment
  - ✓Only 45% of organizations represented in the survey have formal risk assessment and remediation policies in place.
  - ✓Out of institutions with fewer than 2,000 employees, only 31% have such policies.

✓(https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240)

Areas for Improvement

- ✓Sensitive Systems
  - ✓Sensitive systems within higher education were deemed a concern by the SANS group, because there are so many technologies within an education organization.
  - ✓The biggest concerns are administrative systems (selected by 70% of education entities who responded to the multiple-choice survey).
  - ✓Faculty and staff computers, tied with web applications, were the second biggest concerns (selected by 64% of education entities who responded to the multiple choice survey).
  - ✓Faculty and staff mobile devices (selected by 60% of education entities who responded to the multiple choice survey) were the third area of concern.

✓(https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240)

Areas for Improvement

- ✓Sensitive Data
  - ✓Personally identifiable information (PII) receives special attention from respondents to the survey, with 76% having institutional policies restricting access to PII and 71% avoiding storage of PII.

✓(https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240)

Areas for Improvement

- ✓Lack of Encryption
  - ✓Only 54% of respondents to this survey noted their encryption of PII in transit, while just 48% encrypt PII at rest.

✓(https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240)

Areas for Improvement

- ✓Unclassified and Unmanaged Data
  - ✓Only 57% of respondents to the survey classify their sensitive data and provide guidelines.
  - ✓55% define appropriate owner, user and administrative roles.

✓(https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240)

Areas for Improvement

- ✓Staffing and Budgeting
  - ✓While 64% believe they need 1–5 full-time equivalents (FTEs) of additional staff, 43% believe they cannot pay premium rates for premium skills.
  - ✓Lack of budget, selected by 73% of respondents, is deemed a cause of not being able to maintain or increase IT staffing.

✓(https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240)

GEN-16-12

- ✓Dear Colleague Letter issued by the Department of Education.
- ✓Recognizes Cybersecurity as a real threat facing institutions of higher education.
- ✓Acknowledgement that student financial aid information is vulnerable, and valuable to attackers.
- ✓Reminds institutions that under the Program Participation Agreement (PPA) and GLBA, financial aid information must be protected.
- ✓Reminds institutions that under their Student Aid Internet Gateway (SAIG) Enrollment Agreement, they "*[m]ust ensure that all users are aware of and comply with all of the requirements to protect and secure data from Departmental sources using SAIG.*"

GEN-16-12

✓It is advised that important information related to cybersecurity protection is included in the ***National Institute of Standards and Technology (NIST)*** Special Publication 800-171 (***NIST SP 800-171***).

✓Specifically, the ***NIST SP 800-171*** identifies recommended requirements for ensuring the appropriate long-term security of certain Federal information in the possession of institutions.

GEN-16-12

- ✓The Department strongly encourages institutions to review and understand the standards defined in ***NIST SP 800-171***.

- ✓**NIST SP 800-171** is the recognized information security publication for protecting "Controlled Unclassified Information (CUI)," a subset of Federal data that includes unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Federal policies.

GEN-16-12

✓The Department understands the investment and effort required by institutions to meet and maintain the security standards established under ***NIST SP 800-171***.

✓Nonetheless, across the public and private sectors, it is ***imperative*** that organizations continue to ***enhance cybersecurity*** in order to meet evolving threats to CUI and challenges to the security of such organizations.

✓Thus, we ***strongly encourage*** those institutions that fall short of ***NIST*** standards to assess their current gaps and ***immediately*** begin to design and implement plans in order to close those gaps using the ***NIST*** standards as a model.

National Institute of Standards and Technology (NIST)

- ✓Organization under the U.S. Department of Commerce;
- ✓Measurement standards laboratory;
- ✓Developed and released special publication 800-171.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

✓Boiled-down and condensed version of NIST 800-53.

✓Made up of fourteen (14) control families:

Family	Family
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Configuration Protection
Maintenance	System and Information Integrity

✓The families are closely aligned with the minimum security requirements for federal information and information systems described in FIPS Publication 200.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

✓While ***NIST SP 800-171*** is important for protecting ***CUI***, it's also a great data security standard to protect ***PII***, which is something we must protect anyway!

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Access Control***
  - Control family is made up of twenty-two (22) unique controls.
  - The goal of having strong access control is to limit information system access, so that only authorized users, processers acting on behalf of authorized users, or devices (such as other information systems) can access the sensitive data or processes.
  - Practice of the principal of least privilege is ideal when aligning to ***NIST SP 800-171***.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Awareness and Training***
  - Control family is made up of three (3) unique controls.
  - Implementing a strong security awareness program will assist in preventing the exploitation of carbon-based vulnerabilities – your employees.
  - Training is the best control to help users identify malicious emails and infected attachments.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Audit and Accountability***
  - Control family is made up of nine (9) unique controls.
  - Reviewing audit logs is a strong control which assists in the identification of potential malicious activity and detection of anomalous behavior.
  - Audit logs are the first place to go when recovering from an incident in regards to attribution and analysis of impacted areas.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Configuration Management***
  - Control family is made up of nine (9) unique controls.
  - The goal of configuration management is to establish a baseline configuration and inventory of organizational information systems throughout system development life cycles.
  - As new systems are added to a technical infrastructure, understanding baseline configuration policy is key to ensure no required settings are overlooked during implementation.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Identification and Authentication***
  - Control family is made up of eleven (11) unique controls.
  - The identification of information system users, processes acting on behalf of users, or devices is key to understanding what is happening within an information system, and how to better protect it.
  - Without proper identification, there is no protection. Key verticals of a technical infrastructure may be overlooked and under-protected if not explicitly noted.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Incident Response***
  - Control family is made up of three (3) unique controls.
  - The establishment of an operational incident-handling program for organizational information systems, that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, is critical when reducing the impact of an incident.
  - Without a true incident response plan in place, steps to recovery from an incident may be hindered or skipped altogether, increasing the impact of an attack.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Maintenance***
  - Control family is made up of six (6) unique controls.
  - Maintenance on information systems is important to ensure that any recognized-vulnerabilities in software used have been patched, to mitigate the likelihood of an incident.
  - Without patching and general maintenance to systems, the likelihood that an attacker will be able to traverse a network and potentially intercept traffic or sensitive information is higher.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Media Protection***
  - Control family is made up of nine (9) unique controls.
  - The protection of information system media (i.e., physically control and securely store) both paper and digital is important when attempting to limit access to these resources to only authorized personnel.
  - In addition, the sanitization and destruction of this information is crucial to ensure sensitive information cannot be recovered from retired assets.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Personnel Security***
  - Control family is made up of two (2) unique controls.
  - This control discusses the importance of screening individuals prior to onboarding and access provisioning to critical or sensitive information.
  - The insider threat is real, and growing. An in-depth understanding of who really has access to information stored in sensitive areas is of increasing importance.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Physical Protection***
  - Control family is made up of six (6) unique controls.
  - Limiting physical access to systems is important, for many reasons, but mainly surrounding the risk of the insider threat or malicious individuals.
  - Information can be stored on hard-drives, which can easily be stolen. In addition, small external storage devices, such as USBs, can contain malware which would activate when the drive is called upon.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Risk Assessment***
  - Control family is made up of three (3) unique controls.
  - The performance of risk assessment is critical to understanding which systems are of critical risk and contain sensitive information.
  - When accounting for the likelihood and impact of an incident, the results will yield an inherent risk rating. After this rating is produced, controls should be taken into account to return a residual risk.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***Security Assessment***
  - Control family is made up of three (3) unique controls.
  - The assessment of security controls across a technical infrastructure is important to ensure their continued effectiveness.
  - If controls are outdated or are not effective, this could create gaps in security which can be exploited by a malicious individual.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***System and Communications Protection***
  - Control family is made up of sixteen (16) unique controls.
  - The monitoring, control, and protection of organizational communications through the use of architectural designs, software development techniques, and systems engineering principles is important to promote effective information security within organizational information systems.
  - Without an understanding of communication channels, the likelihood that data will be lost or intercepted is greater.

NIST SP800-171

National Institute of Standards and Technology
U.S. Department of Commerce

- ***System and Information Integrity***
  - Control family is made up of seven (7) unique controls.
  - Continued monitoring of uptime of systems and reporting on information system flaws in a timely manner are critical controls related to the survival of the institution.
  - If data processing is halted due to a downed critical system, this could lead to severe financial loss.

NIST SP800-171 (Benefits)

National Institute of Standards and Technology
U.S. Department of Commerce

- ✓ ***Help keep data secure;***
- ✓ ***Cost effective data security standard;***
- ✓ ***It's do-able;***
- ✓ ***Will likely be a requirement down the road.***

What can we do?

- ***Review the control list***
  - It's important to have a solid understand of the requirements within the guideline to ensure that investment is being made in the proper areas.
  - Work with IT, finance, and executive management to create a strategy to map to the special publication.

- ***Call OCD Tech***
  - OCD Tech has assisted a variety of organizations comply with ***NIST SP 800-171***.

What can we do right now?

- ✓***Perform security awareness training;***
- ✓***Implement a strong incident response plan;***
- ✓***Definite critical assets and perform a risk assessment;***
- ✓***Identify and classify sensitive data, know where its stored, and what controls are in place to keep it safe;***
- ✓***Implement a strong cybersecurity and information security program and culture from the top-down.***

The Team

O'Connor & Drew P.C.
Certified Public Accountants

Staff

Michael Hammond– IT Audit & Security Director, with the firm since October 2012.

- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (C|EH)
- Michael is a member of the financial services InfraGard association. A joint partnership between the FBI and private sector.
- Michael is a veteran of the United States Air Force

https://www.linkedin.com/in/michaelwhammond

Staff

Nick DeLena– Senior IT Audit Manager

Nick is the lead senior IT audit manager at O'Connor & Drew. He works in concert with internal senior management to scope and budget engagements. He provides oversight and training to existing staff. Nick's prior engagements includes SOX compliance, SAS70, and FFIEC compliance. In addition to Nick's audit and advisory experience, he also has 12 years in various IT operations and analyst positions.

Certifications and designations:

- Executive Masters in Business Administration (MBA), Brown University
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- CompTIA Security+
- ITIL v3 Foundations Certification (ITILv3F)
- Nick is a member of the science and technology InfraGard association. A joint partnership between the FBI and private sector.

- https://www.linkedin.com/in/nickdelena

Staff

W. Jackson Schultz – Senior Auditor & Consultant

Jackson is a senior auditor and consultant with OCD Tech. Prior to joining the firm, Jackson was a security consultant for a boutique consulting firm with a focus on financial services and HIPAA covered entities. In addition, Jackson has assisted multiple organizations align their governance with NIST SP 800-171. Currently, Jackson performs IT audit control testing for O'Connor & Drew clients.

Certifications and designations:

- Candidate for Executive Masters in Cybersecurity (EMCS), Brown University
- Certified Information Systems Auditor (CISA)
- Jackson is a member of many organizations, such as Information Systems Audit & Control Association (ISACA), Information Systems Security Association (ISSA), InfraGard, a partnership between the private sector and FBI, Cloud Security Alliance (CSA), ISSA New England, and ASIS International.
- Quoted in CIOReview and bankinfosecurity.com

- https://www.linkedin.com/in/w-jackson-schultz-cisa-61902330

Questions?

O'Connor & Drew P.C.
Certified Public Accountants

Thank you!

W. Jackson Schultz, CISA
Senior Consultant – IT Audit & Security
OCD Tech
A Division of O'Connor & Drew, P.C.

e: jschultz@ocd-tech.com
m: (781) 307 8678

O'Connor & Drew P.C.
Certified Public Accountants

OCDTECH