WEDNESDAY'S
News You Can Use

Overview of Cybersecurity Risk for a Government Finance Office

Presented by **Joel Black, CPA &**

Jameson Miller, CPA, CISA

Carl Vinson Institute of Government
UNIVERSITY OF GEORGIA

GGFOA

CPE SPONSORS

Today's Presenters

Joel Black, CPA, is a partner with Mauldin & Jenkins LLC specializing in serving local and state governmental and nonprofit entities throughout the Southeast. He has 24 years of experience providing attestation, consulting and instructional services. Joel currently serves on the AICPA's State and Local Government Expert Panel. His responsibilities have included responding to GASB exposure drafts on behalf of the profession, instructing at national conferences, and updating and re-writing several chapters of the AICPA Accounting and Audit Guide for State and Local Governments and the AICPA Audit Guide on Government Auditing Standards and OMB Circular A-133.

Jameson Miller, CPA, CISA is a Director in the Chattanooga, TN office of Mauldin and Jenkins, LLC. His 12 years of experience includes audits for financial institutions, publicly traded SEC companies, manufacturers, and not for profit organizations. His experience includes Information Systems regulatory compliance reviews and other IT framework audits, SSAE 18 System and Organization Controls (SOC) Audits, and Technical audits and security assessments for computer systems.

Learning Objectives

At the end of this session, you should be able to:

- Identify the types of risks facing local government entities related to cybersecurity and cloud computing
- Recall the basic control frameworks that can be used to mitigate cybersecurity risks
- Recognize best practices and or strategies that can be used to implement and improve information technology controls related to cybersecurity

Current Environment and Trends for Governments

Current Environment for Government

On March 22nd, 2018, officials announced that the City of Atlanta had been affected by a ransomware attack

- A shady hacking group called SamSam was behind the attack
- To fix the damages, the city sought $11.5 million for crisis communications, forensics (looking for what else was still in the system), and extra Information Security Staff
- This attack left multiple city services inoperable for weeks and months
  - Residents could not pay their water bills or traffic tickets along with reporting graffiti or potholes
  - Police officers were forced to write reports by hand
  - The Atlanta Municipal Court could not validate warrants

Current Environment for Government

What exactly occurred?

- SamSam was able to download malicious software onto a device on the city's network
  - This could have been remotely or by a spear phishing attempt
- The software would encrypt and lockdown specified folders and keep the city from accessing them
- A ransom was posted, but shortly taken down, leaving Atlanta to deal with the chaos left behind
- All of the locked files either required hundreds of IT work hours to decrypt, or the files were deleted
  - Any critical data that was compromised had to be "shredded" or securely deleted

Current Environment for Government

There have been attacks that have targeted other governmental entities:

- Over the early months of 2018, the Unique Identification Authority of India (UIAI) has had multiple breaches
  - It's Aadhaar system (contains biometric data, names, addresses, etc.) was infiltrated, resulting in the selling of over 1 billion Indian citizens' personal information on a social media network
- Between July 2016 and October 2017, an Australian national security contractor had been the victim of a cybersecurity breach
  - The attackers ran off with 30 gigabytes of data, which included information on fighter jets, cargo planes, navy ships, and military grade bombs
- On Friday, June 28th, 2017, a Ukrainian website that delivered updates to tax and account software was infected with malware
  - The malware was disguised as ransomware, but would secretly extract and permanently wipe data
  - The attack affected banks, energy firms, senior government officials, and one airport

Current Environment for Government

Other attacks – not just large governments

- On Feb. 25, 2016, a civilian employee in the Sarasota, Fla., Police Department clicked on an attachment to an email
  - Instead of opening a document, the worker inadvertently launched a ransomware attack that encrypted 160,000 city files and triggered an extortion that demanded up to $33 million in the virtual currency known as bitcoin to unlock them
- In Cockrell Hill, Texas, a small city of 4,200, a ransomware attack back in December 2016 encrypted all the files in the police department
  - When the department refused to pay the $4,000 ransom demand, the department's records, dating back to 2009, were lost
- In March 2018, the City of Baltimore's 911 dispatch system was shut down for 20 hours due to ransomware attack

A 2016 survey by the University of Maryland found that more than 25% of local governments across the U.S. faced attempted cyberattacks as often as once or more per hour

Many cybercrimes go unreported because of embarrassment

Cybersecurity Trends

Source of information: Verizon's 2018 Data Breach Investigations Report 11th edition

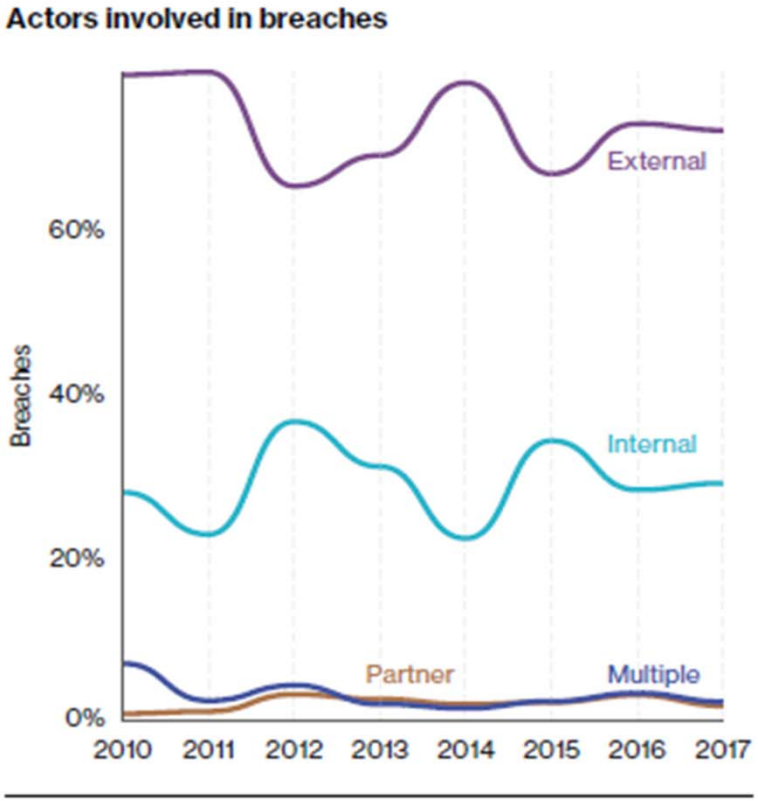


Figure 1. Threat actors within breaches over time

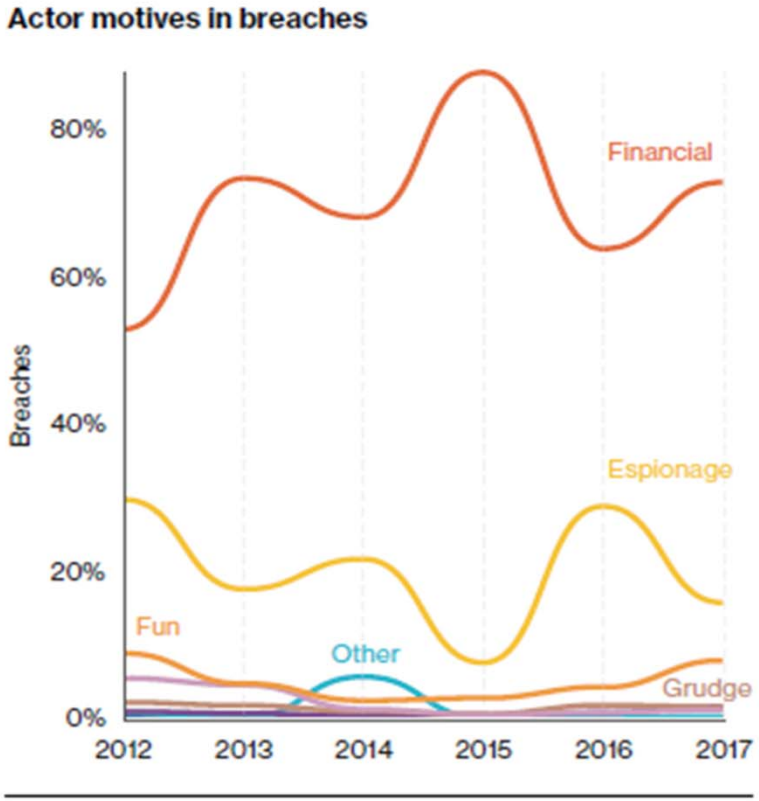


Figure 2. Threat actor motives within breaches over time

Cybersecurity Trends

Source of information: Verizon's 2018 Data Breach Investigations Report 11th edition

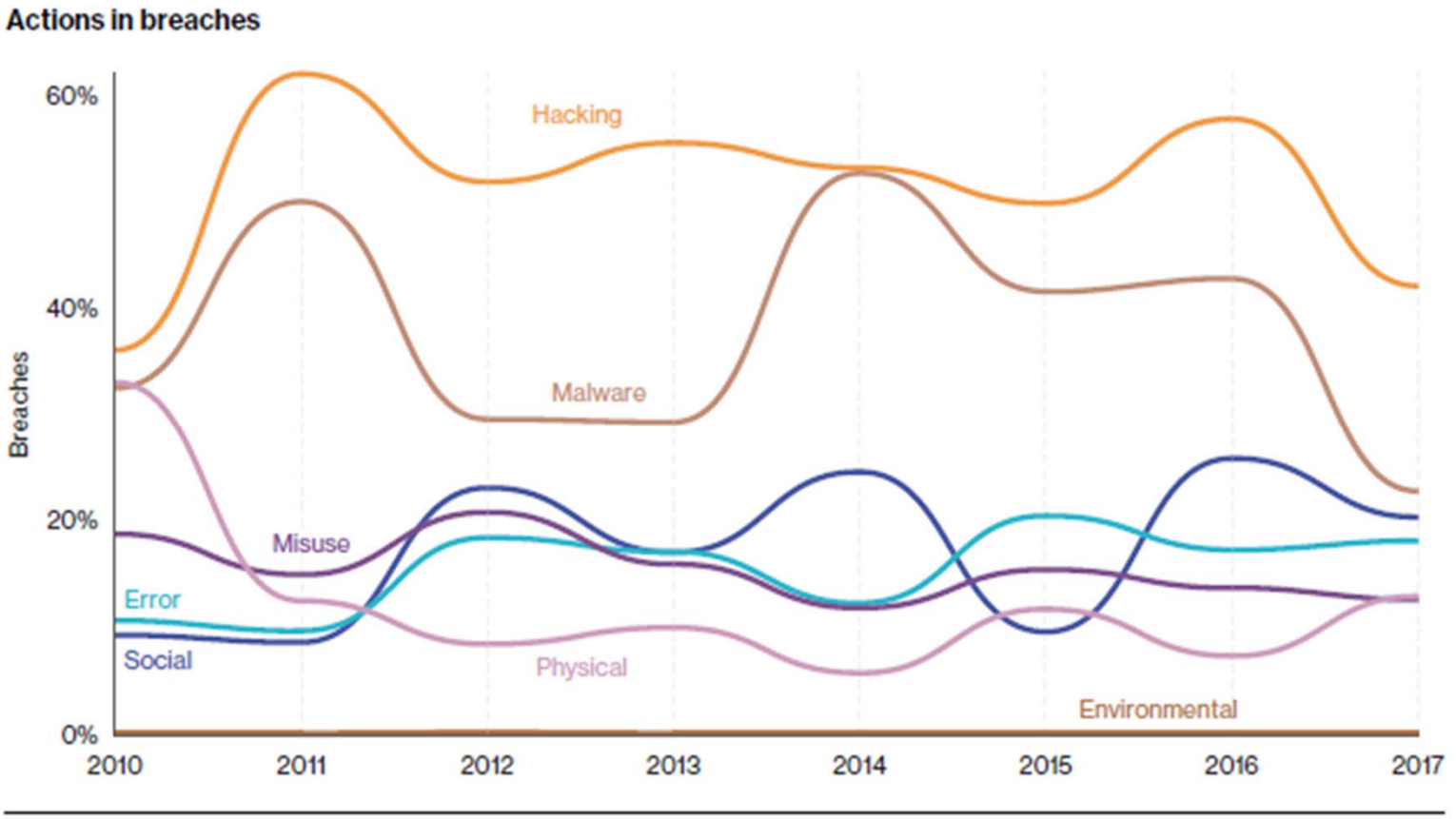
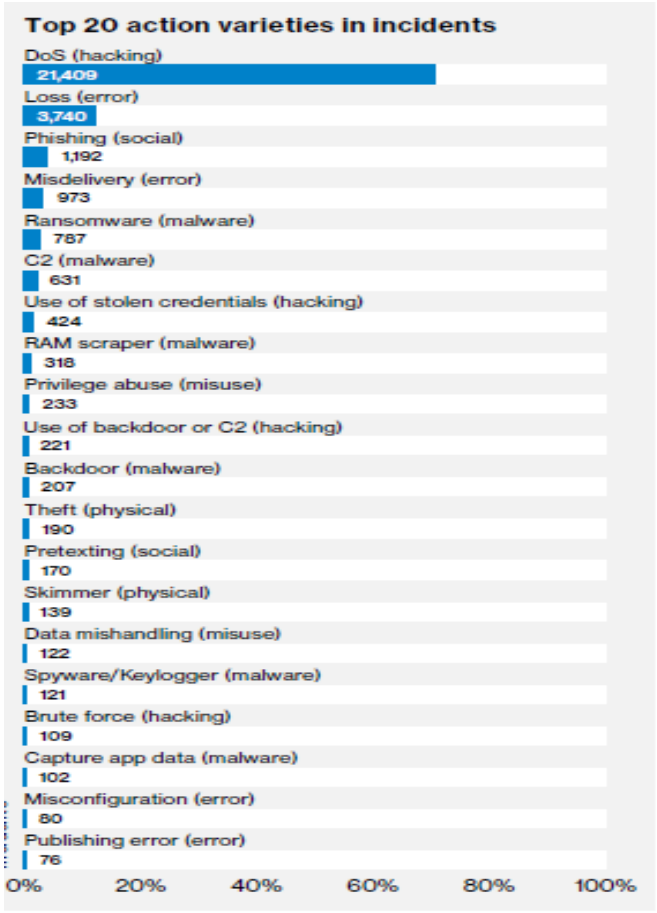


Figure 3. Percentage of breaches per threat action category over time

Cybersecurity Trends

Source of information: Verizon's 2018 Data Breach Investigations Report 11th edition



re 4. Top 20 threat action varieties (incidents) (n=30,362)

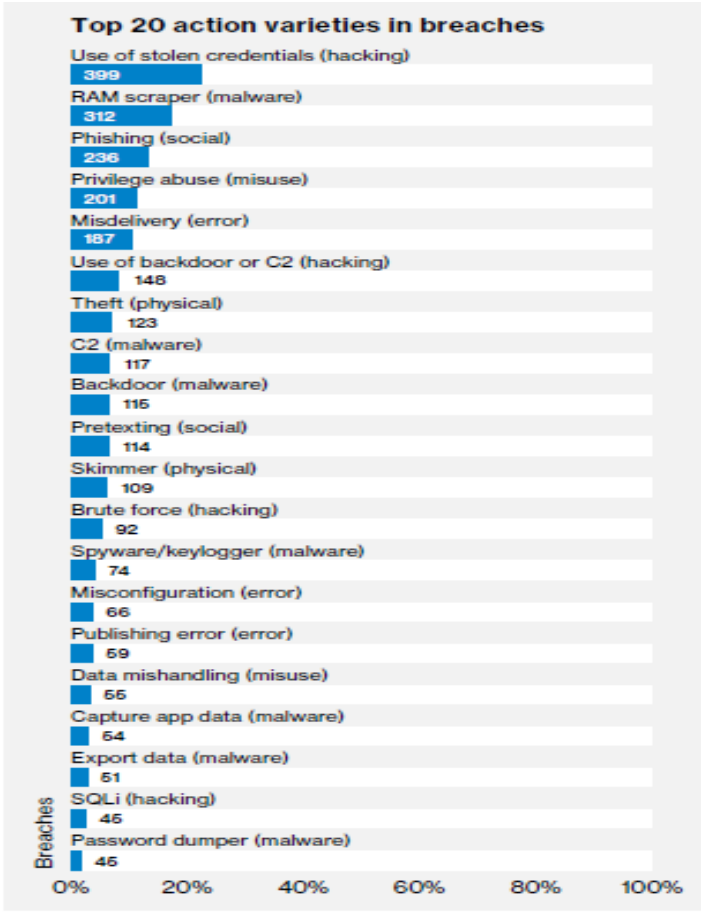
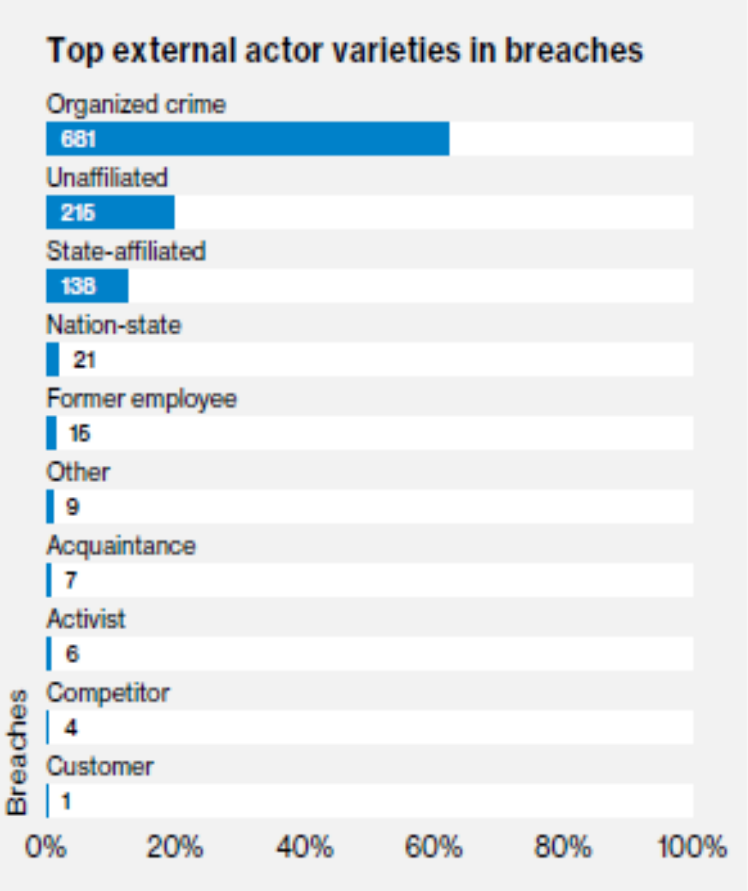
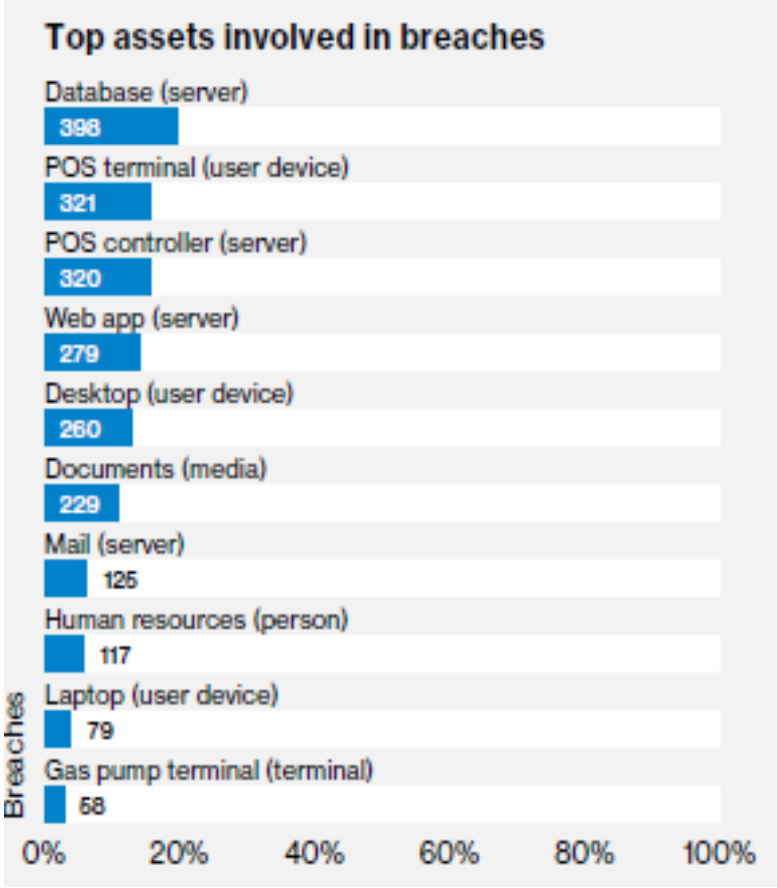


Figure 5. Top 20 threat action varieties (confirmed data breaches) (n=1,799)

Cybersecurity Trends

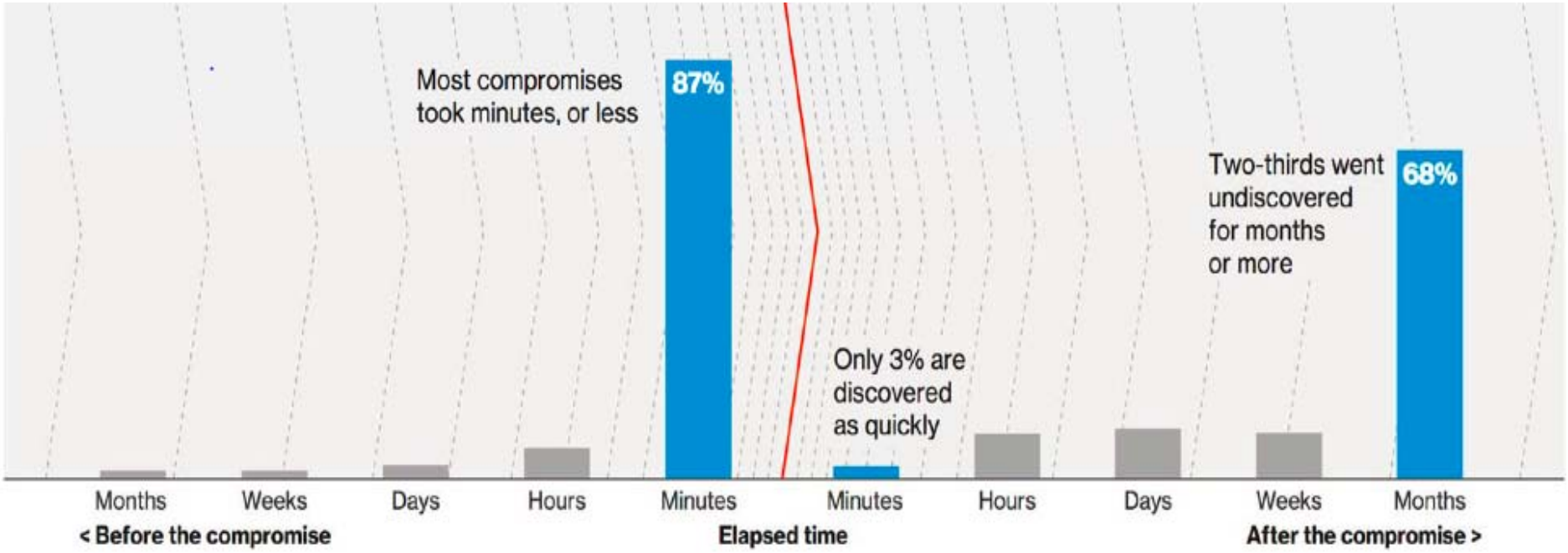
Source of information: Verizon's 2018 Data Breach Investigations Report 11th edition





Cybersecurity Trends

Source of information: Verizon's 2018 Data Breach Investigations Report 11th edition



Knowledge Check

Has your government been the victim of a cyberattack?

A. Yes

B. No

Overview of Risk and Threats

Cybersecurity Risks & Threats:

- Phishing / Spear-Phishing & other Social Engineering
- Network threats
- Mobile threats
- Physical threats
- Internal threats
- Malware, Ransomware, Viruses, etc.
- Insecure web or mobile applications
- Cloud and Vendor risks
- Legal risk

Phishing E-mail Example

---------- Forwarded message ----------
From: **Lindon Breckner** <fnpbrunellajx@outlook.com>
Date: Thu, Jul 26, 2018 at 1:04 PM
Subject: [redacted]
To: "jameson.miller@hlbcpa.com" <jameson.miller@hlbcpa.com>

Lets get right to the point. Neither anyone has compensated me to investigate about you. You do not know me and you're most likely thinking why you're getting this e mail?

Let me tell you, I installed a malware on the xxx streaming (pornography) web-site and guess what, you visited this web site to experience fun (you know what I mean). When you were watching videos, your web browser initiated operating as a RDP having a key logger which gave me access to your display and also web cam. Just after that, my software collected your complete contacts from your Messenger, FB, and e-mail . And then I made a double-screen video. First part shows the video you were viewing (you have a fine taste omg), and second part displays the view of your webcam, & its you.

You have two solutions. We should read up on these choices in particulars:

1st solution is to disregard this e-mail. Consequently, I most certainly will send out your actual video recording to each of your your personal contacts and thus just consider concerning the disgrace you can get. Keep in mind in case you are in an intimate relationship, precisely how it would affect?

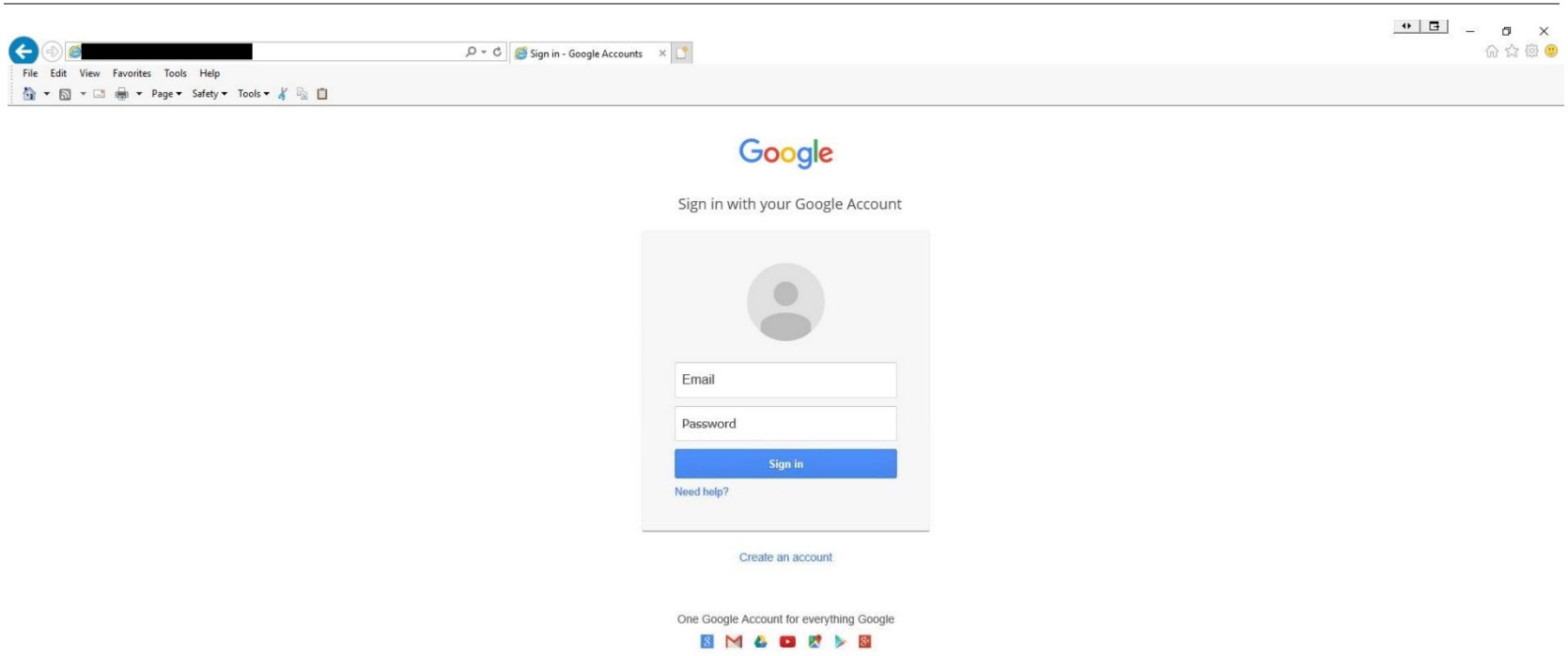
In the second place choice will be to give me $1000. I will call it a donation. In this scenario, I most certainly will right away erase your videotape. You will keep going on your life like this never happened and you will not hear back again from me.

You will make the payment through Bitcoin (if you do not know this, search for "how to buy bitcoin" in Google search engine).

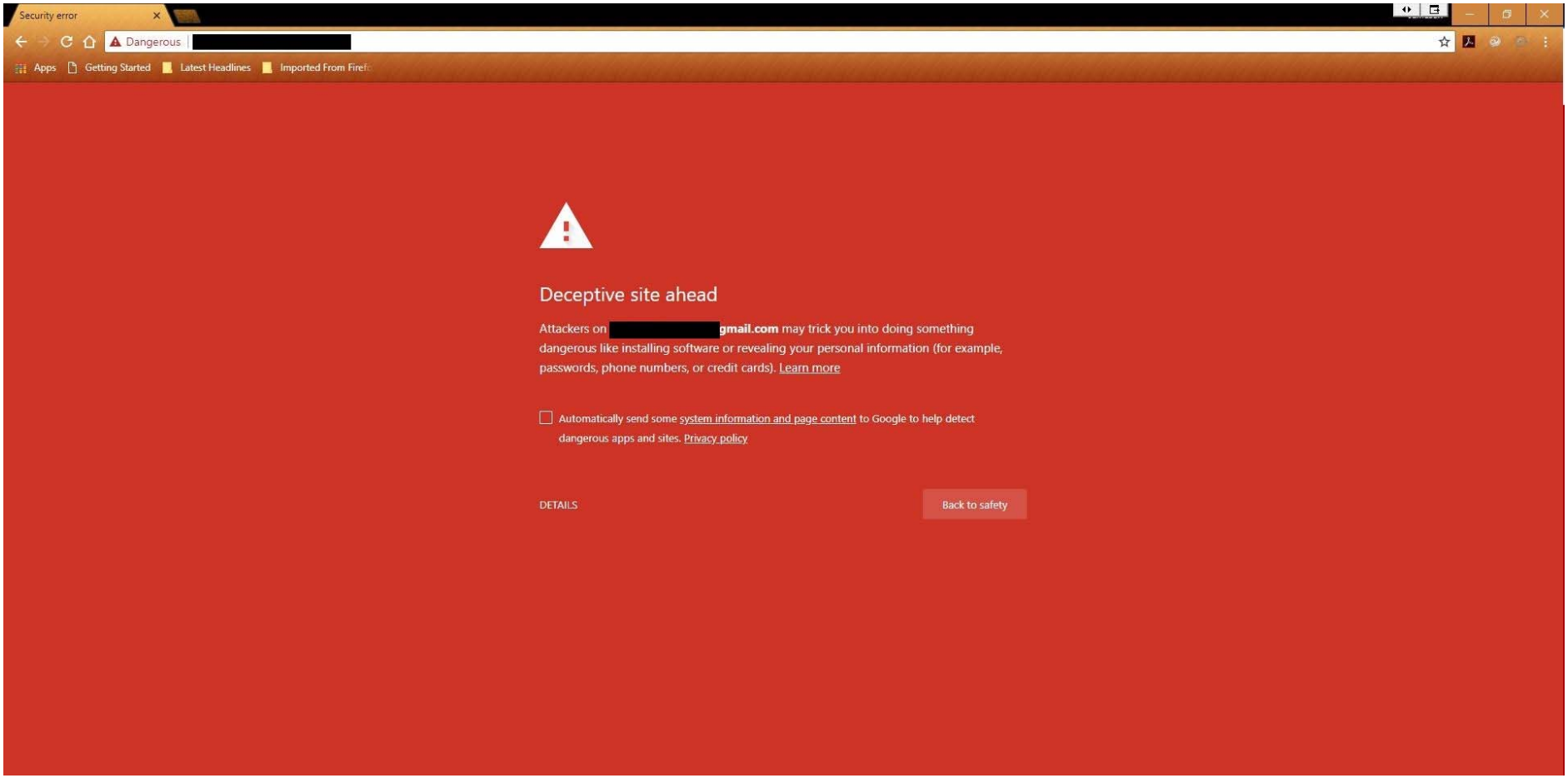
BTC Address to send to: 19qdkhWmTbeaAXYL1tL4WfD9gAWCgJ4jNa
[CASE sensitive, copy and paste it]

Should you are planning on going to the law enforcement officials, good, this email message can not be traced back to me. I have dealt with my moves. I am just not attempting to charge a fee very much, I simply prefer to be compensated. I've a special pixel in this mail, and right now I know that you have read through this email. You have one day in order to pay. If I don't receive the BitCoins, I will definitely send out your video to all of your contacts including close relatives, co-workers, and many others. Nonetheless, if I receive the payment, I will destroy the recording immediately. If you want proof, reply with Yes then I will certainly send your video recording to your 13 friends. This is a non-negotiable offer therefore don't waste my personal time and yours by responding to this e-mail.

Malicious Website Example (IE versus Google Chrome)



Malicious Website Example (IE versus Google Chrome)



Steps to Take to Mitigate Risk

Cybersecurity Risk Management Program (CRMP)

What is a CRMP?

According to the American Institute of Certified Public Accountants (AICPA), a CRMP is a set of policies, processes and controls that are designed to:

- Protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objective, and
- Detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented

Knowledge Check

Does your government have a cybersecurity risk management program (CRMP)?

A. Yes

B. No

What is the purpose of a CRMP?

The AICPA summarizes the purpose of a CRMP using three words:

- **Confidentiality;**
- **Integrity;** and
- **Availability**

What does a CRMP Achieve?

A government entity can be affected by many different types of attacks: Denial of Service, a physical break-in of a device with sensitive information, or through communicative means

Every department of a Government has sensitive data on its employees and citizens (tax billing, utility billing, parks and rec, emergency services, courts, library, payroll, insurance, student portals, etc.)

Attackers have multiple points of entry in breaching a government:

- Social Engineering
- Brute Force
- Malicious software
- Man in the Middle Attacks

What does a CRMP Achieve?

A CRMP ensures a level of protection over an entity's data, information, and systems from these threats and risks by:

- Identifying what needs to be protected;
- Defining threat level;
- Defining risks and threats;
- Defining likelihood of occurrence; and
- Determining the potential impact

What does a CRMP Achieve?

"How do we keep these attacks from happening?"

versus

"How do we stop breaches from occurring, and when they do, what is the most effective procedure to fix it?"

Cybersecurity controls are designed to:

- defend against attacks,
- detect the attacks, and
- react to the attacks

Types of Cybersecurity Controls

Protection Controls

Designed to safeguard against a malicious event or to reduce risk before an actual occurrence

Examples:

- Controls that restrict access to appropriate personnel
- Annual cybersecurity awareness and training controls
- Least-privilege access to data
- Patching Cadence

Types of Cybersecurity Controls

Detection Controls

Designed to discover a malicious event or reduce the risk during or directly after an occurrence

Examples:

- Logging network traffic permitted through the entity's firewall
- Monitoring system changes by having appropriate approving individuals sign off on each change as it occurs
- Identifying vulnerabilities and mitigating potential exposure
- Monitoring user access for both privileged and nonprivileged user accounts
- Security audits for compliance
- Periodic security assessments to identify potential threats.

Types of Cybersecurity Controls

Reaction Controls

Designed to address or reduce risk after a malicious event, occurrence or discovery

Examples:

- Having proper incident response, disaster recovery and business continuity plan and policies in place
- Practicing incident response procedures so that all staff are aware of their roles and action items during a crisis event
- Updating the incident response policies and procedures based on how effective and efficient they were during practice rounds or after real-life events

Cybersecurity is a Business Problem

A cybersecurity risk management program focuses on twelve areas:

- Business Continuity
- Governance
- Risk Management
- Compliance
- Information Security Organization
- Security Policy
- Physical and Environmental Security
- Asset Management
- HR Data Security
- Security communications & Operations
- Access Control
- Systems Development Life Cycle

What is a Cybersecurity Framework (CSF)?

A cybersecurity framework is a policy framework based on computer security that helps to improve an entity's ability to prevent, detect, and respond to any threats

- The AICPA's CRMP is a comprehensive type of CSF
- Other cybersecurity framework examples:
  - National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
  - International Organization for Standardization (ISO) 27001 & 27002
  - SANS Institute Center for Internet Security (CIS) Critical Security Controls
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Control Objectives for Information and related Technologies (COBIT 5)
  - Hi-Trust CSF

Knowledge Check

A control that restricts access to appropriate personnel is known as a….

A. Detection control

B. Protection control

C. Reaction control

D. Position control

AICPA's Cybersecurity Risk Management Reporting Framework

Developed to:

- Assist organizations with communicating relevant and useful information about the effectiveness of their CRMP
- be flexible as it's related to the scope of the engagement – (Business units, segments of function of an entity)

A key component of the AICPA's recently released System and Organization Controls (SOC) for Cybersecurity Report

AICPA's SOC for Cybersecurity

- Based on two complementary sets of criteria:
  - Description Criteria
  - Trust Services Criteria (Control Criteria)
- Designed to be non-restricted, publicly available use report
- The purpose is to help senior management, boards of directors, analysts, investors, and business partners gain a better understanding of an organization's Cybersecurity efforts
- Controls from commonly used CSFs have been mapped to the Control Criteria

Cybersecurity External Advisory Services Available

- Information Security Risk Assessments
- HIPAA Security Assessments
- Vulnerability Assessment
- Penetration Testing
- Application Security Assessment
- Information Security Policy Development
- Database Security Assessment
- Network Device Configuration Reviews
- Social Engineering Assessments
- Information Security Awareness Training
- Security Incident Response Program Development & Testing
- Disaster Recovery and Business Continuity Plan Consulting
- Readiness Assessments for SOC Reporting – (SOC 1, 2, 3 and SOC for Cybersecurity)

Other Items

Cloud Computing

Cloud computing is the practice of using a remote network of servers to store, manage, and process data over the internet, rather than using a local server or a personal computer

There are many benefits that an entity will have with cloud computing:

- Working remotely
- Transferring data seamlessly
- 24/7 Data access
- Focus on core infrastructure versus computer infrastructure and maintenance

Cloud Computing Risk

Common Cloud Computing risks:

- Cloud computing provider does not have to meet an entity's legal needs
- If the cloud computing provider is breached, then any organization that uses the service is breached
- Cloud computing may not encrypt every piece of information
- If the provider undergoes an outage, the user's entire organization may be suspended until the system is back up
- Data caps can limit an entity's bandwidth and amount of storage

Cloud Computing Vendors should be evaluated as part of an Entity's Vendor Management Program and risks/threats should be considered within Risk Assessment documentation

Managing Cloud Computing Risk

- Considered within the entity's Risk Assessment
- Evaluated as part of a structured Vendor Management Program
- Clearly defined scope of services
- Identified and measurable data management requirements
- Service level agreements
- Restriction of access to authorized providers and/or entity personnel
- Back-up and disaster recovery strategies
- Review System and Organization Controls (SOC) or other third party assurance reports

Cybersecurity Compliance Requirements

- All 50 States have enacted legislation for notice of individuals of breach of PII
  - *NIST 800-122 defines PII as, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individuals identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."*
- Federal Breach Notification Requirements – Privacy Act, the Federal Information Security Management Act, Office of Management and Budget Guidance, the Veterans Affairs Information Security Act, HIPPA, the Health Information Technology for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, the Fair Credit Reporting Act

Impact of General Data Protection Regulation (GDPR)

- General Data Protection Regulation (GDPR) applies to:
  - Organizations based in the EU that process the personal data of natural persons; and
  - Organizations that do not have a branch in the EU, but who offer goods and services to individuals residing in the EU and who processes the personal data of EU residents
- Regulation went into effect May 25th, 2018
- Emphasizes "Privacy by Design"
- GDPR is not just an EU specific regulation – Every EU citizens' private data regardless of where it is stored, must be protected
- Includes Data Breach Notification Requirements
- Designed to work with popular IT/Cybersecurity frameworks

Impact of (GDPR)

- Financial costs of non-compliance will add up and may include:
  - Regulatory fines – Up to 4% of annual worldwide revenues or €20 million, whichever is higher
  - Fees to defend lawsuits
  - Infrastructure repair/redesign
  - Public Relations deflection of negative comments
  - Hiring compliance contractors to process data on your behalf
  - Overtime labor costs for addressing incidents
  - New/updated security tools

Knowledge Check

A formal risk assessment is not necessary for a cloud computing vendor since the vendor is contractually responsible for data management.

A. True

B. False

GDPR Key Takeaways

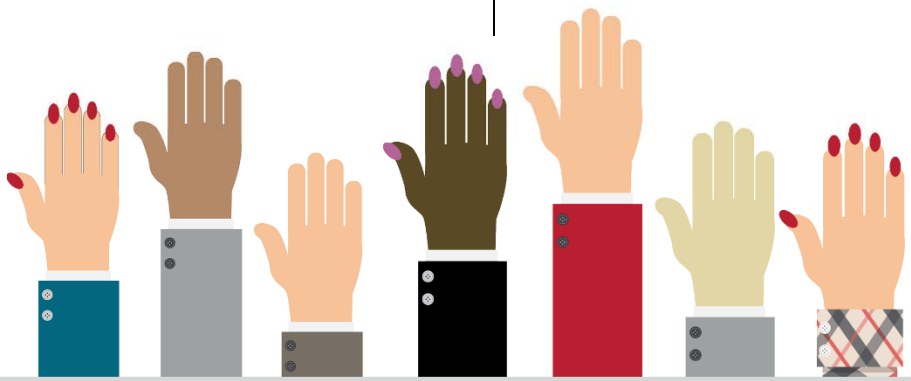
- Global Impact – Even U.S. companies need to evaluate the impact
- Only 29% of organizations were fully GDPR-compliant by the deadline
- 1 in 10 didn't know whether his/her organization is required by law to be GDPR-compliant
- The top five challenges in preparing for GDPR compliance:
  - Data Discovery and Mapping
  - Prioritizing GDPR compliance among business priorities
  - Organizational education and change programs
  - Ensuring cross-departmental collaboration and buy-in
  - Preparation for data subject access or deletion requests

Source: ISACA GDPR Readiness Survey, May 2018

QUESTIONS?

Joel Black – jmblack@mjcpa.com

Jameson Miller – jmiller@mjcpa.com



Thank You!

Carl Vinson
Institute of Government
UNIVERSITY OF GEORGIA

Since 1927, the Carl Vinson Institute of Government has been an integral part of the University of Georgia. A public service and outreach unit of the university, the Institute of Government is the largest and most comprehensive university-based organization serving governments in the United States through research services, customized assistance, training and development, and the application of technology.

GGFOA

The mission of the Georgia Government Finance Officers Association is to promote and foster excellence in governmental financial management through programs that enhance the abilities, knowledge and influence of the government finance professional.

CPE SPONSORS

The University of Georgia, Carl Vinson Institute of Government is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.NASBARegistry.org.

Connect With Us!

facebook.com
/VinsonInstitute

facebook.com
/GGFOA

Carl Vinson
Institute of Government

Government Finance
Officers Association

@CVIOG_UGA

@GGFOA