



Government

BKD
CPAs & Advisors

Everyone needs a trusted advisor. Who's yours?



Current Issues in Cybersecurity



OUR GOALS FOR TODAY

1

Current Cyber Threats and Trends

2

Advancements in the Industry

3

10 Things Auditors Should Know
About Cybersecurity

What Makes the Public Sector So Vulnerable?

- Breadth of staff skills
- Broad regulatory exposure
- Shared infrastructure
- Silos
- Budgetary challenges
- Technology-focused

CYBER THREATS



**\$6.0
Trillion**
Cost of cyber crime damage by 2021.

Cyber Threats

- The practice of injecting malware into software updates increased by 200% during 2017.
- The number of web application vulnerabilities increased by 212% in 2017.
- There was a 54% increase in mobile malware during 2017
- In February 2018, there was one phishing attempt in every 3,331 emails and one piece of malware for every 645 email.
 - That means that in an organization of 500 email users who receive a median of 100 emails per day, the security infrastructure will receive 15 phishing attempts and 77 pieces of malware each day.
- While the massive ransomware campaigns we saw in 2015 and 2016 have abated to some extent, we continue to see targeted ransomware campaigns focused on specific industries like healthcare and **government**, among others.

Osterman Research. Best Practices for Protecting Against Phishing, Ransomware and Email Fraud, April 2018.



Cyber Threats

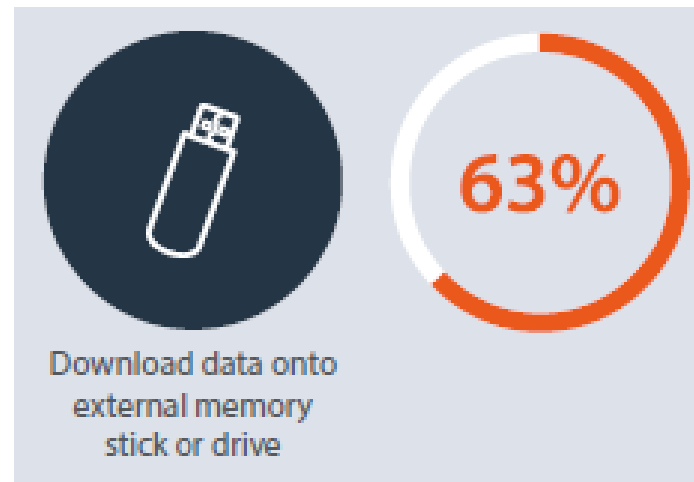
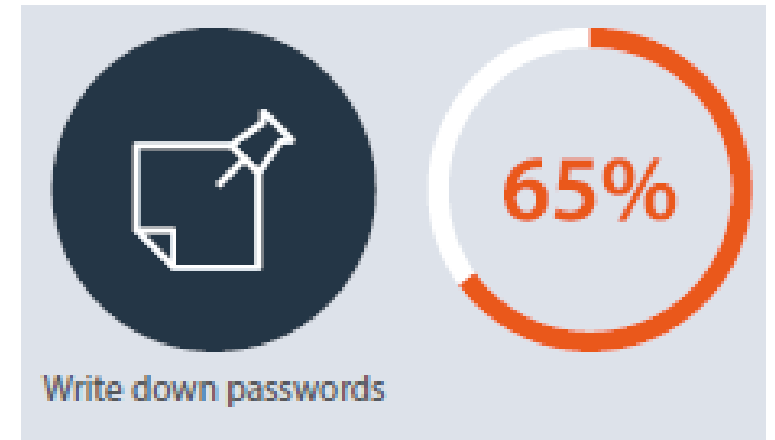
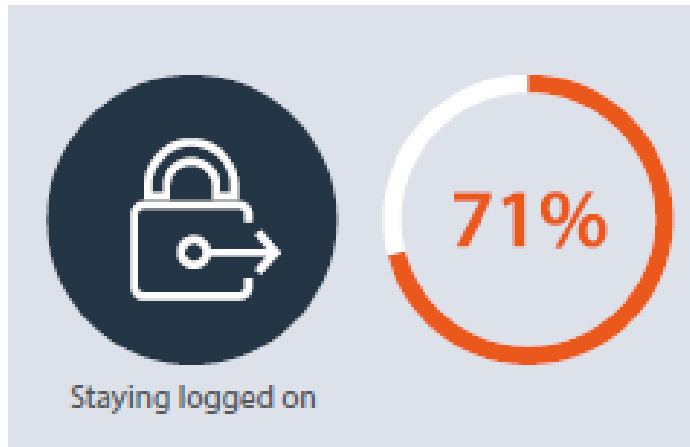
- The biggest threats to your assets are actually from the same old threats that we were worried about last year, five years ago, and in many cases even a decade ago.
- Only a handful of attacks truly use sophisticated “Mission Impossible” techniques.
- When a criminal is trying to hack an organization, they won't re-invent the wheel unless they absolutely have to.
- Cyber criminals tend to seek the highest returns in the shortest time with the least risk.
- Cyber criminal organizations are successful because they are generally well funded, they have the technical resources to create new and increasingly more capable attack methods, and they often are highly collaborative in nature

Cyber Threats

- According to IBM's "Cyber Security Intelligence Index" 95% of all security incidents **prey on human weakness** in order to lure insiders within organizations to unwittingly provide them with access to sensitive information.
- 59% of respondents agree that most information technology security threats that directly result from insiders are the result of **innocent mistakes** rather than malicious abuse of privileges.

Cyber Threats

INSIDER RISKS



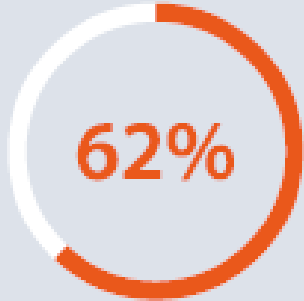
Bogmar Privileged Access Threat Report 2018

Cyber Threats

INSIDER RISKS



Send files to personal email accounts



Log on over unsecured WiFi



Tell colleagues passwords



Cyber Attacks to Watch Out For

1. Phishing
2. Pretexting
3. Baiting
4. Quid Pro Quo
5. Tailgating
6. Ransomware

Phishing

- Phishing is the crafting of a message that is sent typically via email and is designed to influence the recipient to “take the bait” via a simple mouse click.
- Seek to obtain personal information, such as names, addresses and social security numbers.
- That bait is most often a **malicious attachment** but can also be a link to a page that will request credentials or drop malware.

Phishing

- May use **link shorteners** or embed links that redirect users to suspicious websites in URLs that appear legitimate. (Bitly, TinyURL, Ow.ly, etc.)
 - From: <https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/>
 - To: <https://ibm.co/1PO3b9x>
- Fake/disposable e-mail address generators
 - Yahoo Mail, Dispostable, GuerrillaMail, SpamBog, GMX, etc.
- Messages tend to incorporate **threats, fear and a sense of urgency** in an attempt to manipulate the user into acting promptly.

Phishing

- Some phishing emails are more poorly crafted than others to the extent that their messages oftentimes **exhibit spelling and grammar errors.**
- In a normal (median) organization, **78% of people don't click** a single phish all year. That's pretty good news.
- In average in any given phishing campaign **4% of people will click it**--the vampire only needs one person to let them in.
- **Only 17% of phishing campaigns were reported.** Additional training should also be bestowed on users that don't report the phishing!

Phishing examples

This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] 10:24 AM
To: [redacted]
Cc: [redacted]
Subject: Your account has been limited

**1. Fake sender domain.
(not service@paypal-australia.com.au)**

2. Suspicious Subject and content.

3. Bad grammar

4. Hovering over link reveals suspicious URL.

PayPal™

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm <http://69.162.70.169/ppau/> the account, and then follow the instructions.
Click to follow link

[Log in your account now](#)

PayPal Email ID PP32260008777636

Phishing examples

From: Carole [redacted] [mailto:[redacted]]
Sent: Monday, October 12, 2015 9:46 AM
To: Jerry [redacted]
Subject: Request
Importance: High

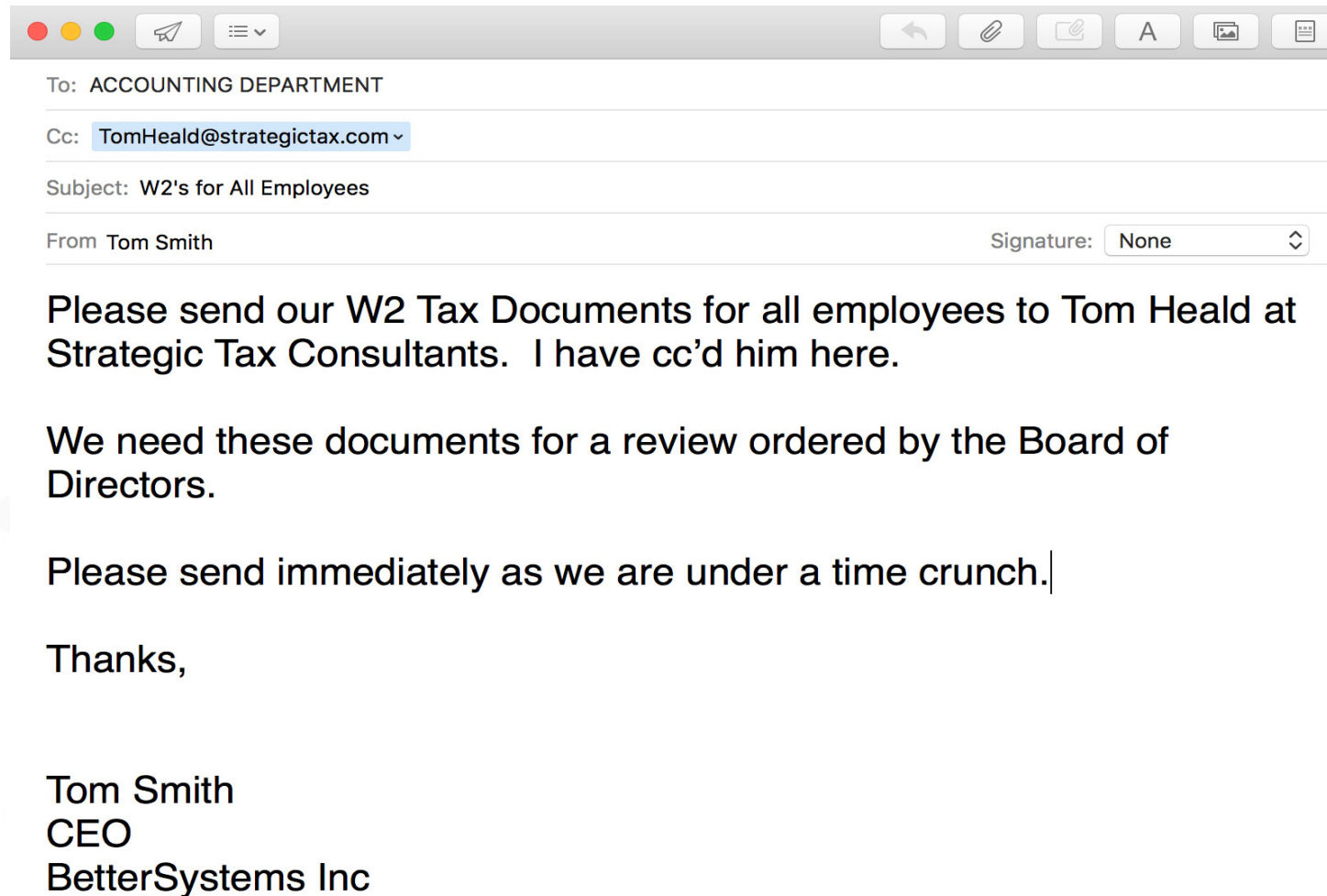
Hello Jerry,

I need you to facilitate a wire transfer for a payment, let me know if you're available and I will forward the details for the payment. I'll wait for your email.

Thanks.

Carole [redacted]

Phishing examples



PRETEXTING

- Pretexting is the **creation of a false narrative** to obtain information or influence behavior.
- Could be a phone call, text message, email, etc. designed steal the victims' personal information.
- Scammer pretends that they need certain bits of information from their target in order to confirm their identity.
- Pretexting may also involve impersonating co-workers, police, bank, tax authorities, clergy, insurance investigators, auditors, etc.

PRETEXTING

- The pretexter must simply prepare answers to questions that might be asked by the victim.
- In some cases, all that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet to create a pretextual scenario.
- Unlike phishing emails, which use fear and urgency to their advantage, pretexting attacks rely on **building a false sense of trust** with the victim.
- The attacker may develop a relationship and even help the victim execute the exploit.

EMAIL-BASED PRETEXTING example

From: "Bank of America" customerservice@bankofamerica.com
To: "Jane Smith" jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required



Dear Customer,


At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, [sign up now](#). New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department 



Phone-BASED PRETEXTING examples

- New credit card.
- Past due bill/collection call.
- Delinquent taxes.

Baiting

- Baiting is the promise of an item or good that hackers use to entice victims to get login credentials to a certain site.
- Baiting attacks are not restricted to online schemes. Attackers can deliver malware via the use of physical media.
- Many people will pick up USBs and plug them into their computers without thinking.
- The USBs may automatically activate a keylogger that allows access to observe an employee's online activity and login credentials or install malware.



Quid Pro Quo

- The Quid Pro Quo usually **assumes the form of a service**, whereas Baiting frequently takes the form of a good.
- One of the most common types of quid pro quo attacks involve fraudsters who impersonate IT service people and who spam call as many direct numbers that belong to a company as they can find.
 - These attackers offer IT assistance to each and every one of their victims.
 - Eventually you will reach someone with a legitimate problem.
 - The user will be grateful you called and will eagerly follow your instructions.
 - The fraudsters will promise a quick fix in exchange for the employee disabling their anti-virus program that assumes the guise of software updates.
 - The attacker then gets the user to install malware on their computer.

Tailgating

- Another social engineering attack type is known as tailgating or “piggybacking.”
- These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area.



Ransomware



- Attacks are inevitable.
- Around half of business victims pay the ransom.
- Most are able to retrieve data after payment.
- Many would pay again.
- Ransomware will continue to be one of the most prevalent attacks.
- Perpetrators are being greatly assisted by the emerging **Ransomware as a Service (RaaS)**

Telstra Security Report 2018.

Ransomware

- **City of Atlanta, GA (Mar 2018)**
 - Five of Atlanta's 13 government offices were "hijacked". What made Atlanta such an easy target – even for a relatively common form of ransomware – was its incredibly outdated use of technology--old computers running on non-supported platforms. Cost to date **\$2.7 million**.
- **Colorado Department of Transportation (Feb-Mar 2018)**

SamSam ransomware morphed into something new and reinfected CDOT computers that had already been cleaned. In April, 80% functionality had been restored at an estimated cost of up to **\$1.5 million** after a computer virus forced the department's back-end operations offline.
- **City of Leeds, AL (Mar 2018)**

Paid **\$12K** in bitcoin to remove lock.

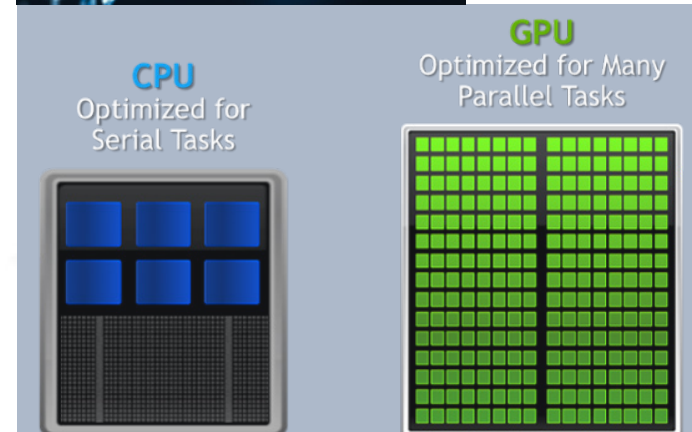
According to the Telstra Security Report 2018, four out of five ransomware victims who paid a ransom to recover their files said they would pay the ransom again to recover data if no backup files are available.

Recommendations - Basics

- **Inventory**

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?

Tangible Assets	Intangible Assets
Equipment	Trademarks
Machinery	Franchises
Buildings	Copyrights
Vehicles	Licenses
Stock	Goodwill
Land	Patents
Cash	Brands



Recommendations - Basics

- **Educate**

- Technology is no substitute for employee education.
- Educate and re-educate the entire organization, not just IT.
- Include the Board, Executives and Vendors.
- Knowledge is power.
- Do not discourage false-positive reporting.
- Document your security policies in a knowledge database so that everyone understand exactly what is going on – and why.
- Develop and rehearse a robust incident response program.



Recommendations - Basics

- **Patch**

- Applications
- Databases
- Operating systems – servers, workstations, etc.
- Anti-virus/Anti-malware – engines and signatures.
- Third-party applications.

Recommendations - Basics

- **Limit**

- Control use of administrative privileges.
- Limit access based on need-to-know (least privilege).
- Limit and control remote access.
- Do not share credentials. Consider a password safe.
- Consider multi-factor authentication.
- Limit the use of portable media.
- Be situationally aware for potential physical security issues.
- Make your trash unattractive to dumpster divers.
- Consider disabling macros.

Recommendations - Basics

- **Check**

- Lock down everything that is not needed.
- Generate logs and review them. Don't forget to document your review.
- Escalate potential security issues.
- Limit and monitor vendor access.
- Filter out suspicious email addressed to employees.
- Implement a policy for dealing with suspected phishing and pretexting.

Recommendations - Basics

- **Prevent**

- Lock your laptop whenever you are away from your workstation.
- Do not give out personal or company confidential information on the phone, through the mail or over the Internet unless you have initiated the contact or know who you are dealing with.
- Monitor in and outbound traffic for unusual patterns.
- Encrypt data at rest and in motion. Don't just protect the perimeter (firewall), also protect the data.
- Segment critical data. Encrypt data within crown-jewel segments.

Recommendations - Basics

- **Backup**

- Implement a regularly scheduled backup program that meets your business and records retention requirements.
- Put some distance between your primary and secondary sites.
- For critical applications, perform a full restoration or fail-over test at least annually.
- Backup and restore **not only data, but also the applications.**
- Understand the differences between cloud storage and cloud backup.

Cyber Trends for 2018

Experian projects the top data breach trends of 2018 include the following:



Data Breach
Industry Forecast
2018

- The United States may experience its first large-scale attack on critical infrastructure, causing chaos for governments, companies and private citizens.
- Failure to comply with new European Union regulations will result in large penalties for U.S. companies.
- Perpetrators of cyberattacks will continue to zero in on governments, which could lead to a shift in world power.
- Attackers will use artificial intelligence (AI) to render traditional multifactor authentication methods useless.
- Vulnerabilities in internet of things (IoT) devices will create mass confusion, leading to new security regulations.

Advancements in Industry

- Content filtering
 - Ingress
 - Egress
- PhishAlarm
- Nothing beats good old fashion training!
- At one point, cyber was a race with companies getting ever more and complex tools. Some of that is still true however focus has been placed more on improved security awareness and incident response.

10 Things Auditors Should Know

1. Leverage existing frameworks/ guidelines

- Auditors should consider mapping of the NIST “Framework for Improving Critical Infrastructure Cybersecurity” to ISO27001:2013 controls and COBIT 5 to reduce the scope of the audit, hence, making the audit more manageable.

2. Consider forthcoming legislation

- Auditors should study how forthcoming and existing legislation could potentially be incorporated into cyber security programs (GDPR, PCI-DSS).
- Auditors need to understand the global regulatory environment and the differences that can exist between geographic regions.

10 Things Auditors Should Know

3. Understand what qualifies as a risk

- All risks are subjective. To qualify as a “risk” a threat needs to be associated with a vulnerability that, if exploited, could negatively impact an information asset. If it does not, it is not a threat.

4. Recognize that users pose the biggest security risk

- To contribute tangible results, auditors should prioritize people over product. Cyber security education is the silver bullet

10 Things Auditors Should Know

5. Basic information security controls still hold true

- As part of overall security (including cyber security), these controls provide a valid baseline of security controls that help enforce security-in-depth (e.g., physical & logical access controls, application of “principle of least privilege”).

6. Ensure a cyber incident response policy is in place

- Auditors need to assess whether a proper crisis management and communication plan is in place and clearly communicated and tested as appropriate.

10 Things Auditors Should Know

7. **Cyber security strategy needs to be agile – landscape is “mutating”**

- Strategy needs to be adaptable and scalable to handle new attack methods. Cannot assume that what currently keeps your IT environment secure will continue to remain secure indefinitely.

8. **Cyber security awareness depends on the right training**

- Employees need sufficient and timely education and training to help combat the ever-changing cyber security threat. Security needs to be interwoven into the fabric of an organization.

10 Things Auditors Should Know

9. Everything is connected to everything

- The primary function and objective of any cyber device is connectivity. Devices are like climbers roped together on the side of a mountain — if one falls it can bring down anything connected to it. Need for a holistic cyber security view. It's imperative that auditors understand and address the bigger picture.

10. Be aware of credential theft techniques

- Auditors should have knowledge of credential theft attack techniques (e.g. pass-the-hash, key logging, token impersonation, and man-in-the-middle attacks).

What is the right AMOUNT of security?



Questions?

Rhonda Plantenga, ITRS Managing Director

303-861-3545

rplantenga@bkd.com

Thank You!