Building a Culture of Information Technology Security from the Top Down

Charlie Grantham

MTMSERVICES

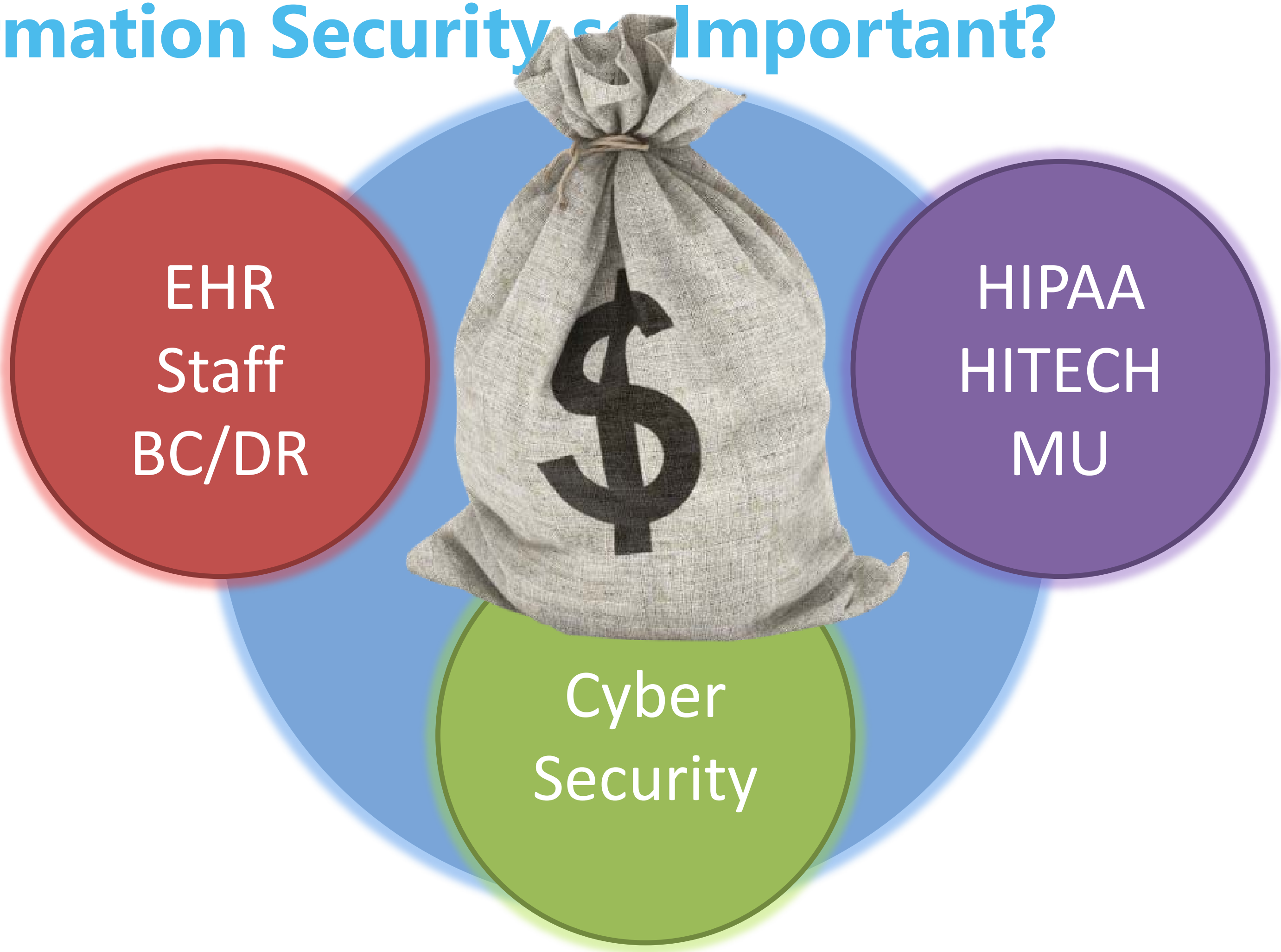
IT and Process Optimization Consultant

charlie.grantham@mtmservices.org

910-734-3141

www.mtmservices.org

Why is Information Security so Important?



Internal Concerns

EHR
Staff
BC/DR

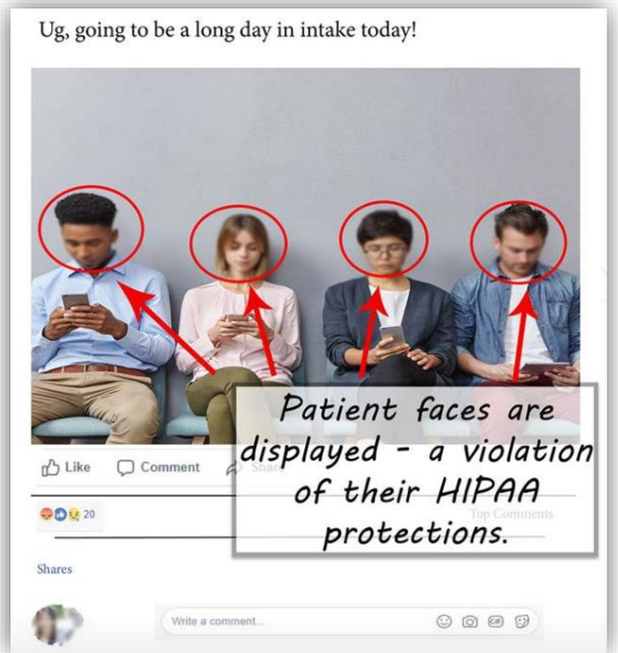
HIPAA
HITECH
MU

Regulatory Concerns

Cyber Security

External Concerns

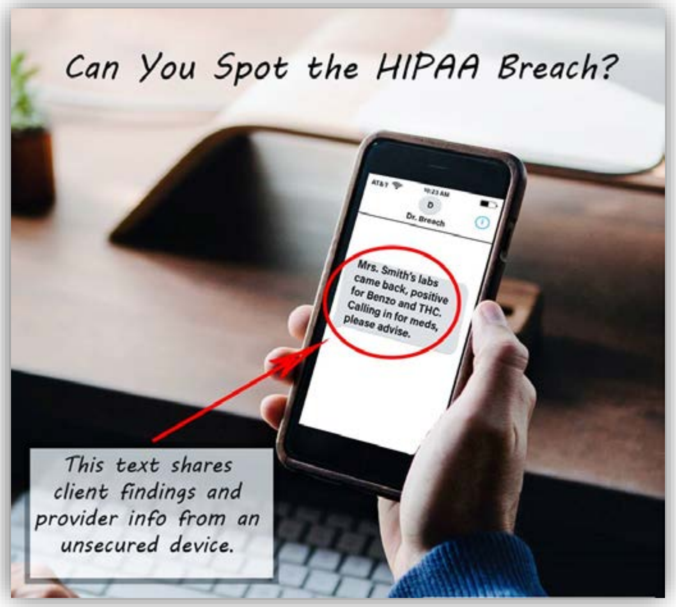
Building a Culture of Information Technology Security from the Top Down


Ug, going to be a long day in intake today!

Patient faces are displayed - a violation of their HIPAA protections.

Internal Concerns

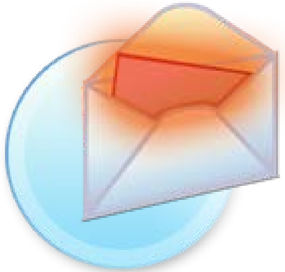
HIPAA compliant


Can You Spot the HIPAA Breach?

Mrs. Smith's labs came back, positive for Benzo and THC. Calling in for meds, please advise.

This text shares client findings and provider info from an unsecured device.

Building a Culture of Information Technology Security from the Top Down



External Concerns

Building a Culture of Information Technology Security from the Top Down

Regulatory Concerns

HealthIT.gov
SM

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA ·

Building a Culture of Information Technology Security from the Top Down

Creating a Culture of Information Technology Security throughout the organization

A Great place to start down the road to Security is utilizing the Security Risk Assessment as a guide.

- Information Security Policies
- Workstation/Laptop Security
- Mobile Media Security
- Wireless Security
- Malware Protection
- Configuration Management
- Vulnerability Management
- Secure Disposal
- External Breach Protection
- PHI Transmission Protection
- Password Management
- Access Control and Monitoring
- Remote Access and Authentication Control
- Training and Awareness
- Third Party Security Management
- Incident and Breach Response
- Business Continuity Management
- Auditing
- Physical and Environmental Security

Understanding YOUR scope

- Assess
  - Determine your risks using the SRA as a guide.
- Roadmap
  - Develop a plan that moves forward with attainable goals.
- Implement
  - Commit to the plan and support project leaders.
- Reflect
  - Increased knowledge after implementations and continual process improvement lead to better workflows.

Examples of Administrative Safeguards

- A1 - § 164.308(a)(1)(i) **Standard** Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its electronic protected health information (ePHI)?
- A39 - § 164.308(a)(5)(ii)(A) **Addressable** As part of your practice's ongoing security awareness activities, does your practice prepare and communicate periodic security reminders to communicate about new or important issues?
- A64 - § 164.308(b)(3) **Required** Does your practice execute business associate agreements when it has a contractor creating, transmitting or storing ePHI?

Examples of Physical Safeguards

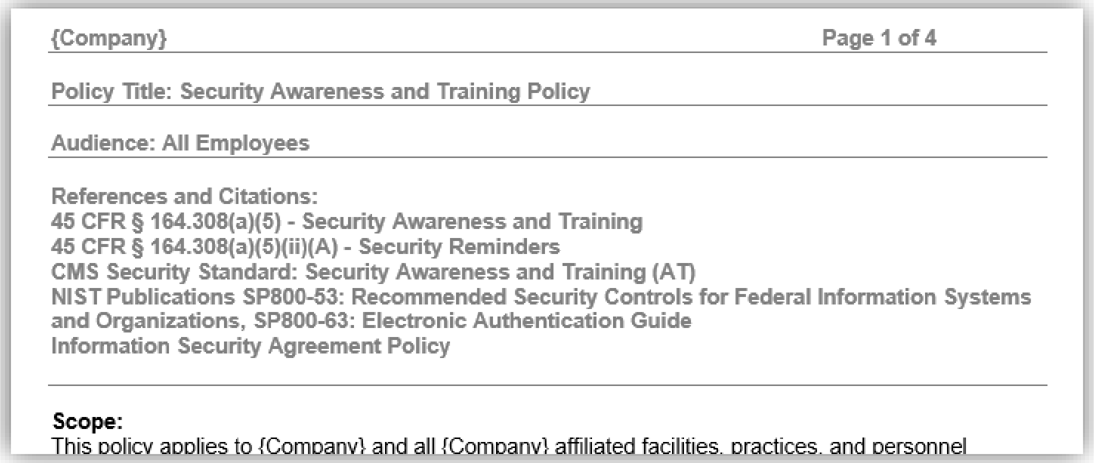
- PH1 - § 164.310(a)(1) **Standard** Do you have an inventory of the physical systems, devices, and media in your office space that are used to store or contain ePHI?
- PH6 - § 164.310(a)(2)(i) **Addressable** Have you developed policies and procedures that plan for your workforce (and your information technology service provider or contracted information technology support) to gain access to your facility and its ePHI during a disaster?
- PH31 - § 164.310(d)(1) **Standard** Do you remove or destroy ePHI from information technology devices and media prior to disposal of the device?

Examples of Technical Safeguards

- T1 - § 164.312(a)(1) **Standard** Does your practice have policies and procedures requiring safeguards to limit access to ePHI to those persons and software programs appropriate for their role?
- T17 - § 164.312(a)(2)(iii) **Addressable** Does your practice have policies and procedures that require an authorized user's session to be automatically logged-off after a predetermined period of inactivity?
- T28 - § 164.312(b) **Standard** Does your practice have policies and procedures for creating, retaining, and distributing audit reports to appropriate workforce members for review?

Importance of Policies and Procedures

- “It didn’t happen if you don’t write it down.”
- Clearly define boundaries via policies and procedures.
- Build auditable trails.
- Reference regulations in policies when possible.



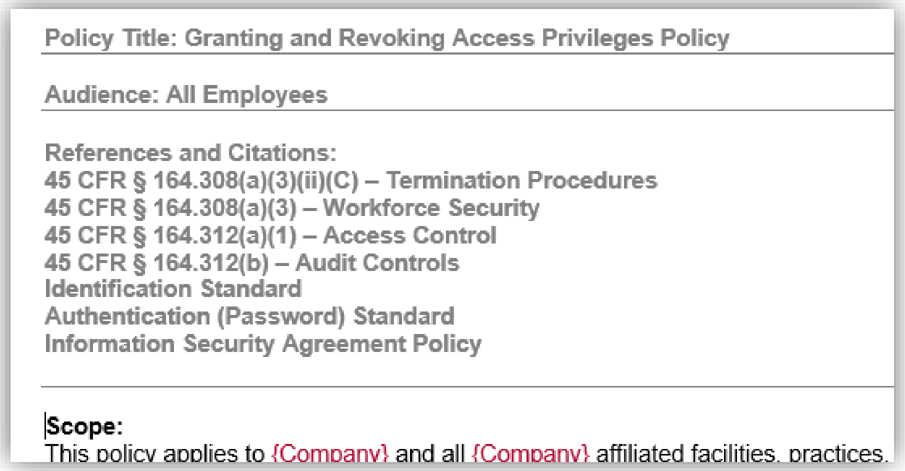
{Company} Page 1 of 4

Policy Title: Security Awareness and Training Policy

Audience: All Employees

References and Citations:
45 CFR § 164.308(a)(5) - Security Awareness and Training
45 CFR § 164.308(a)(5)(ii)(A) - Security Reminders
CMS Security Standard: Security Awareness and Training (AT)
NIST Publications SP800-53: Recommended Security Controls for Federal Information Systems and Organizations, SP800-63: Electronic Authentication Guide
Information Security Agreement Policy

Scope:
This policy applies to {Company} and all {Company} affiliated facilities, practices, and personnel



Policy Title: Granting and Revoking Access Privileges Policy

Audience: All Employees

References and Citations:
45 CFR § 164.308(a)(3)(ii)(C) – Termination Procedures
45 CFR § 164.308(a)(3) – Workforce Security
45 CFR § 164.312(a)(1) – Access Control
45 CFR § 164.312(b) – Audit Controls
Identification Standard
Authentication (Password) Standard
Information Security Agreement Policy

Scope:
This policy applies to {Company} and all {Company} affiliated facilities, practices,

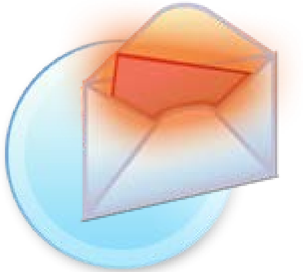
Staff Training – Constant Reinforcement

- Create a Security Awareness Program.
- Monthly HIPAA Walkthroughs.
- Security Training at Orientation, along with additional “Online Learning/CE” required of all employees yearly.
- Simulated phishing attacks.
  - Follow-up training required for repeat offenders.
- Mass emails warning about specific phishing attacks (including ransomware).

Cyber Security

Hoaxes

E-mail sent by online criminals that tries to trick you into giving them money



Spam

Unwanted e-mail, instant messages, e-cards, and other online communication

Identity Theft

A crime where con artists get your personal information and access your cash and/or credit

Cyber Security

Viruses/Ransomware

Software programs designed to invade your computer, and copy, damage or delete your data

Root kits/Trojans

Viruses that pretend to be programs that help you while destroying your data and damaging your computer

Spyware/Malware

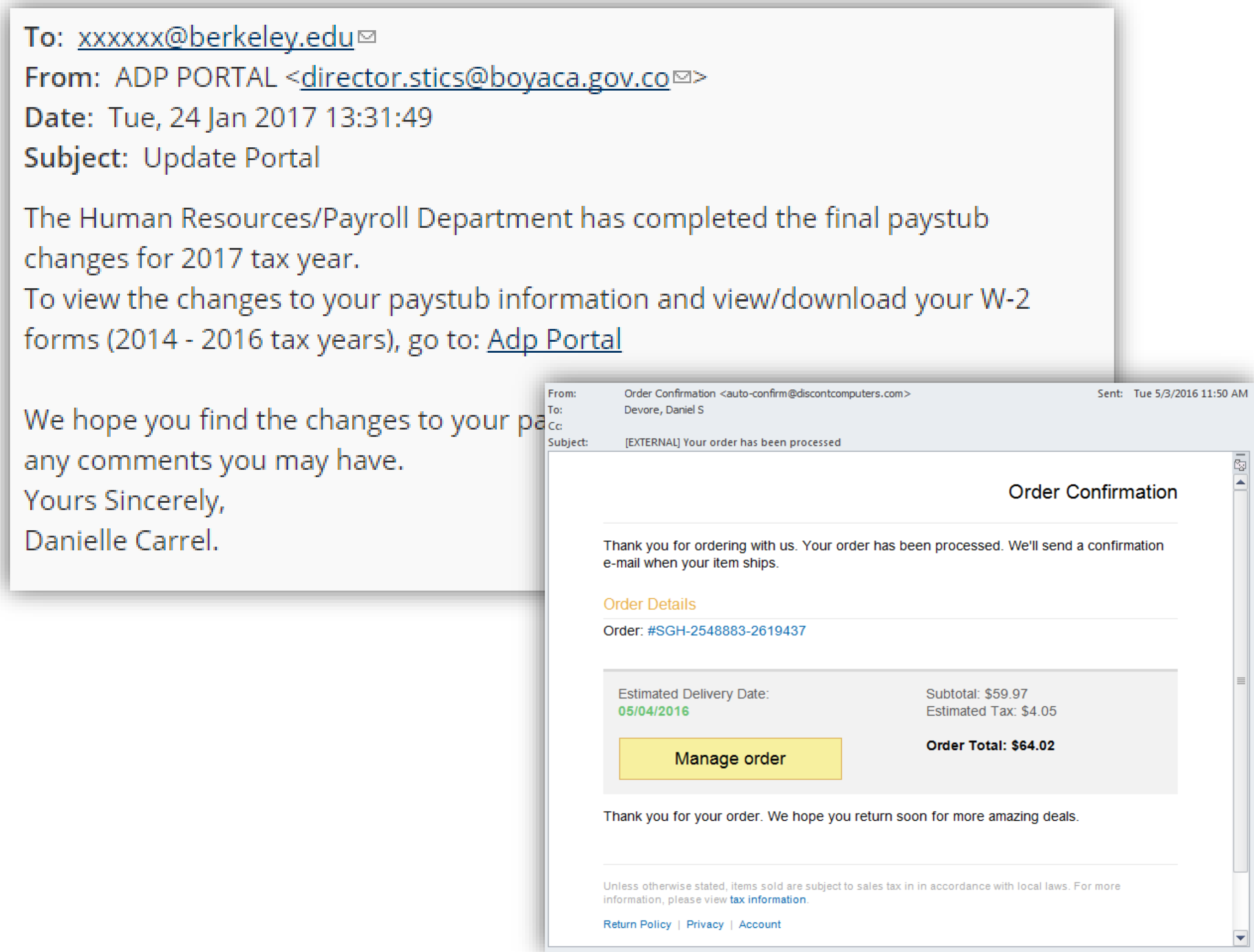
Software that secretly watches and records your online activities or sends you endless pop-up ads

Phishing

- Currently the most common attack
- Things to look for:
  - Spelling errors and Grammar
  - Check the address
  - Formatting errors
  - Smell Test

Phishing

- When in doubt… DELETE
- Think (hover and read) before you click
- Not all are obvious
- Spearfishing / Whaling
- When in doubt… DELETE



To: xxxxxx@berkeley.edu
From: ADP PORTAL <director.stics@boyaca.gov.co>
Date: Tue, 24 Jan 2017 13:31:49
Subject: Update Portal

The Human Resources/Payroll Department has completed the final paystub changes for 2017 tax year.
To view the changes to your paystub information and view/download your W-2 forms (2014 - 2016 tax years), go to: Adp Portal

We hope you find the changes to your pa
any comments you may have.
Yours Sincerely,
Danielle Carrel.

From: Order Confirmation <auto-confirm@discontcomputers.com>
Sent: Tue 5/3/2016 11:50 AM
To: Devore, Daniel S
Cc:
Subject: [EXTERNAL] Your order has been processed

Order Confirmation

Thank you for ordering with us. Your order has been processed. We'll send a confirmation e-mail when your item ships.

Order Details

Order: #SGH-2548883-2619437

Estimated Delivery Date: 05/04/2016

Subtotal: $59.97
Estimated Tax: $4.05

Order Total: $64.02

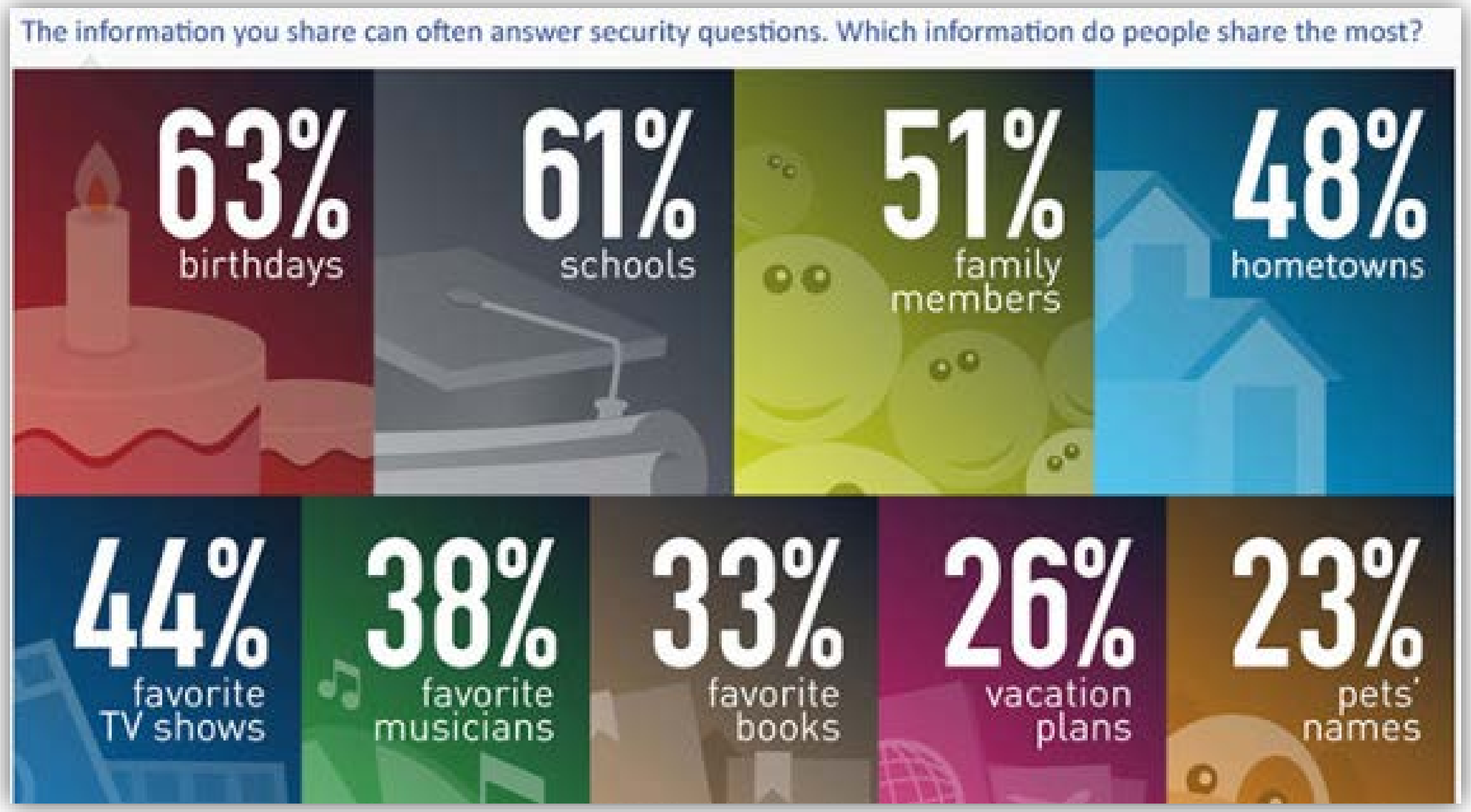
Thank you for your order. We hope you return soon for more amazing deals.

Unless otherwise stated, items sold are subject to sales tax in in accordance with local laws. For more information, please view tax information.

Return Policy | Privacy | Account

Social Media

- Cyber Criminals often use information shared by you, against you.



The information you share can often answer security questions. Which information do people share the most?

Disaster Recovery and Business Continuity

- Inability to access your clients information is a both a clinical and a security risk.
- Be Prepared.
- Prioritize systems.
- Develop and Test your Plans.

Internal Business Silos Can be a Security Concern

Examples of Silos creating IT Security issues:

- Renovation/Layout changes of Clinical Areas without Information Security Considerations.
- New Contract for Copiers negotiated.
- Clinical staff implements Collaborative Documentation without proper safeguards.
- Departmental only software/hardware decisions.

Defeating Internal Silos

- Almost all purchases now have a technology component, some minor, some major.
- Get input/direction from IT/Security/Compliance from concept to purchasing to implementation.
- Value IT’s opinion more (or at least as much) as the salesman's.
- Deploying technology against the will of your IT department can be challenging but is sometimes necessary.
- Security and Compliance costs money, so spend it wisely and try and cover as many “bases” as possible with your purchases.

Technical Staff

- Staff retention for technical staff can pay big dividends
  - Have enough staff
  - Invest in your equipment and infrastructure
  - Invest in your technical staff's education
  - New hire orientation can be lengthy and costly in production and losses of functionality
  - Remember to tell them thanks

Questions?