CYBERSECURITY
PREPAREDNESS

Are you ready?


Are you prepared for this?

How about this?

WHAT WE **THINK** WE **LOOK LIKE** TO AN ATTACKER

WHAT WE **REALLY** LOOK **LIKE** TO AN ATTACKER

services (web/mail/dns)

web applications (java, php, .net)

people (employees, customers)

TODAY WE'LL FOCUS ON **PEOPLE**

THE PEOPLE **"PROBLEM"**

1. What We Have
    - Firewall Controls
    - Spam Controls
    - IPS Controls
2. What We Need
    - Human Controls

THE PEOPLE **"PROBLEM"**

1. Employees/Users – The Weakest Link
2. Reasons for breaches:
    1. Human Error - misconfigurations
    2. Poor Password Practices
    3. People are far too trusting..."not going to happen to me"

SOCIAL **ENGINEERING**

SOCIALENGINEERING

METHODS

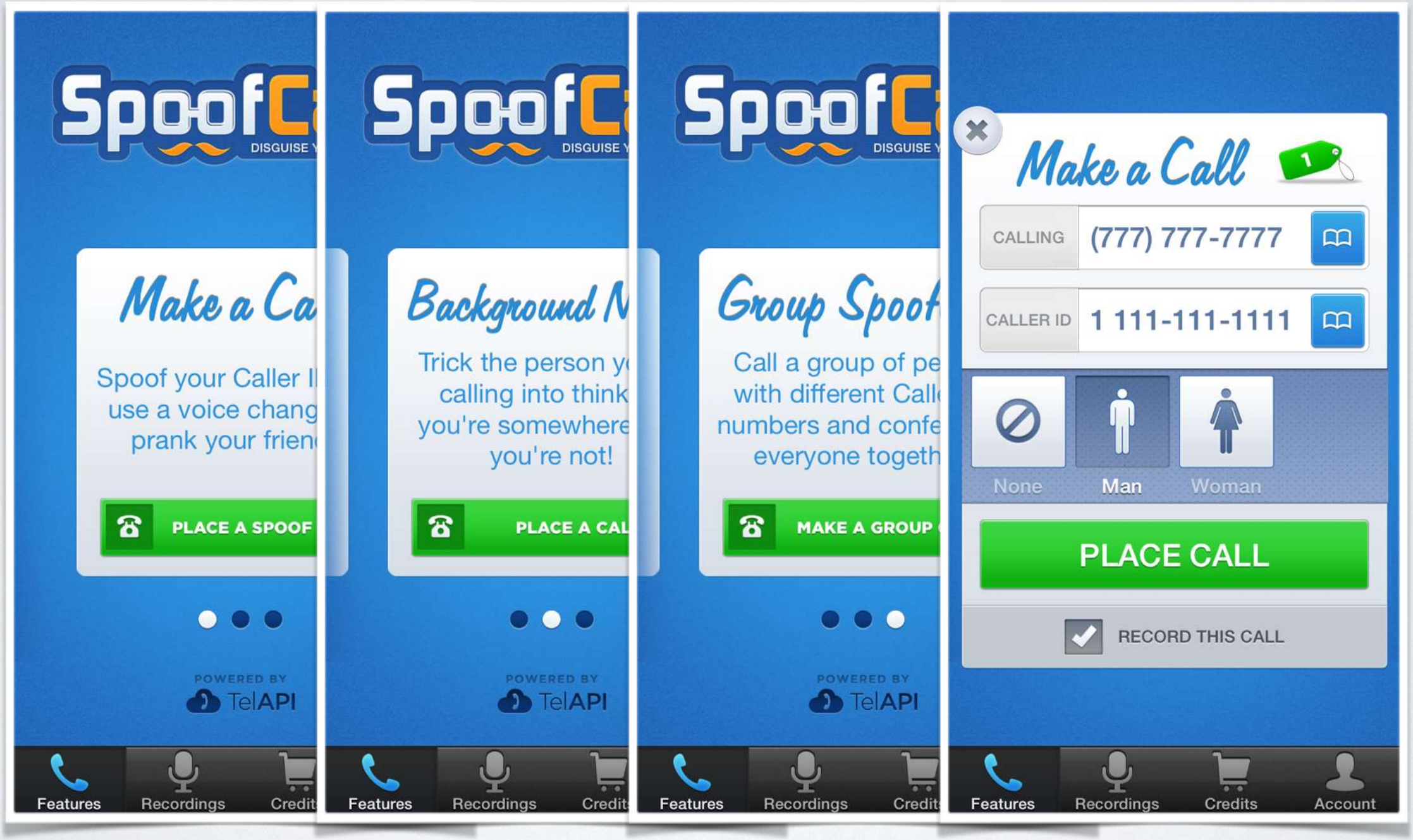
- Physical
- By phone (vishing)
- By email (phishing

SOCIALENGINEERING
PHYSICAL

- Casing the joint
- Watching the people
- Lock picking
- Watching vendors
- Piggybacking

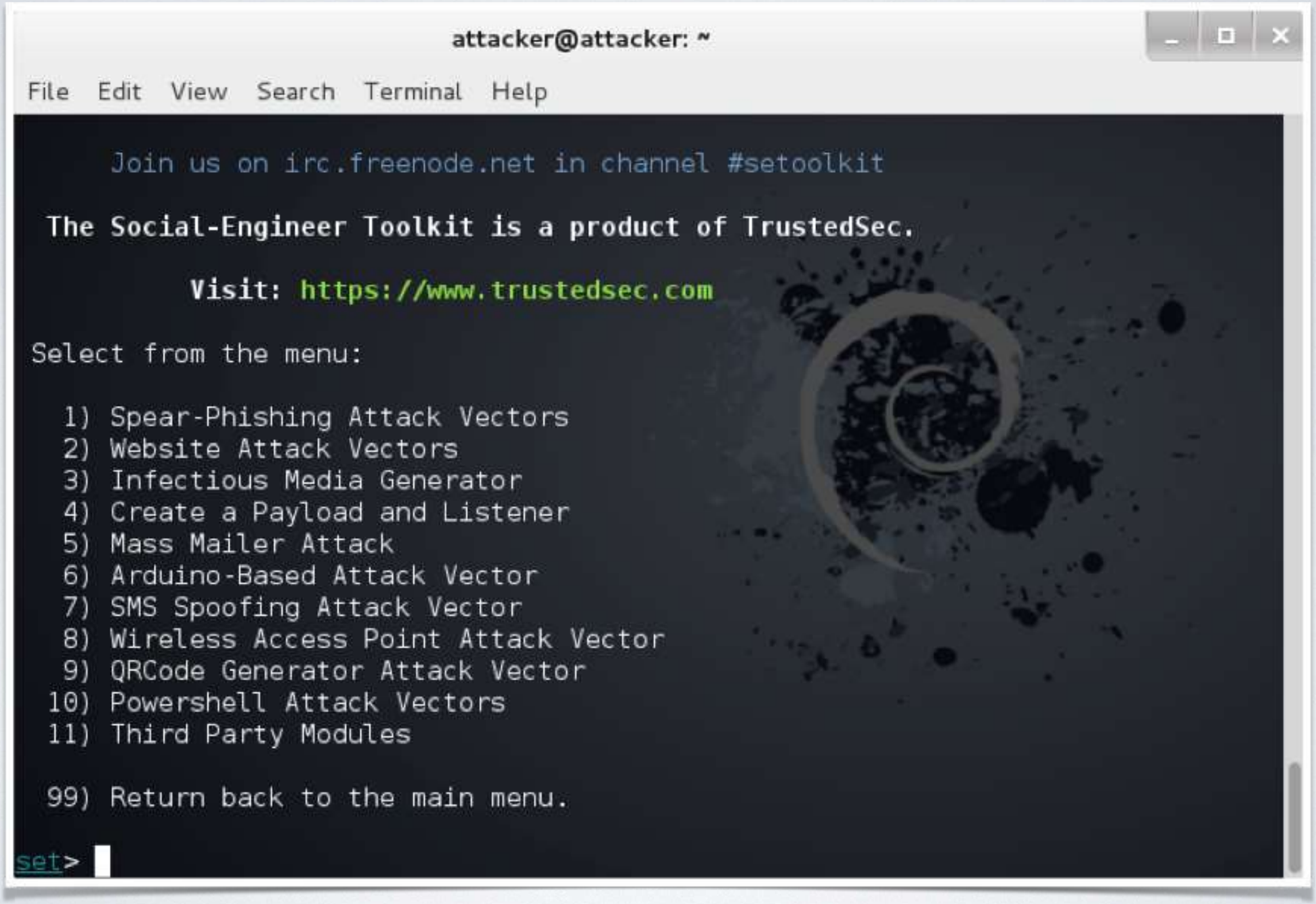
SOCIALENGINEERING

VISHING



SOCIALENGINEERING PHISHING

SOCIALENGINEERING PHISHING



ENTER.....SECURITY AWARNESS

IMPORTANCE OF SECURITY **AWARENESS**

Security breaches can cause serious damage to your organization (and EVERYONE needs to be aware):

1. Financially
2. Reputation
3. Loss or theft of customer information
4. Loss of time recovering from a breach

IMPORTANCE OF SECURITY **AWARENESS**

Also, it's an opportunity to:

1. Raise enterprise-wide discussions on risk.
2. Get security out of the inner dungeon of IT and into the hands of the end user
3. Create an environment that helps remind people of the "secure thing" to do

…so…what exactly is security awareness?

SECURITY **AWARENESS**

...is the **knowledge and attitude** members of an organization possess regarding the **protection** of the physical and informational **assets** of the organization.

...once Armed with an understanding of the risks, they can better define **how to better protect** the systems and data.

DEVELOPING A **SECURITY AWARENESS PROGRAM**

DEVELOPING SECURITY **AWARENESS**

Risk & Needs Assessment

1. Training is based on risks specific to your organization
2. Determine data, processes, and activities relevant to your organization
3. Create security Awareness training based on the previous two steps

DEVELOPING SECURITY **AWARENESS**

1. Posters, flyers, email communications as an on-going basis
2. Program should be measurement for success
3. Employees can easily report incidents
4. Get employer buy-in
5. Develop training relevant user and data types

CHALLENGES YOU'LL FACE

CHALLENGES

1. Employees
    1. People can be resistant to change
    2. Employees view it as extra work
    3. Employees can lose access to systems
2. Time to implement
3. Leadership buy-in
    1. No immediate visible return on investment
4. Limited Budget

Report predicts more healthcare cyber and ransomware attacks in 2017

The healthcare industry will be a target for cyber attackers in 2017 while the nefarious practice of holding patient records for ransom will be an industry scourge, according to predictions by credit reporting firm Experian.

“Personal medical information remains one of the most valuable types of data for attackers to steal,” according to the 10-page report, the company's fourth annual data breach forecast.

Keeping Sanford Safe in the DIGITAL AGE

SANFORD HEALTH

WHAT VENDORS WHERE?

- Do you know which existing vendor users are connected to your network and what types of access they have?
- Start by identifying and documenting your existing vendors and 3rd parties.

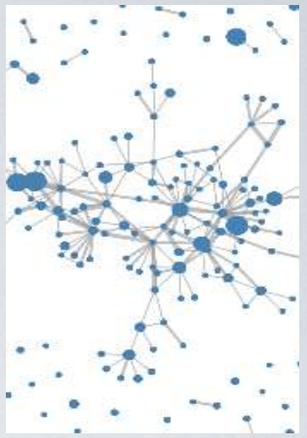
ACCESS PLAN?

- Documentation and reporting facilitates oversight, accountability, monitoring, and risk management.

- Define a policy and procedure to monitor and report.

1. **Define clear roles and responsibilities** for overseeing and managing the relationship and risk management process.
2. **Access to the network** – will they have to use certain connection methodologies? Will their accounts be active or inactive with process for turning on when needed?
3. **Collect contact information** for the vendors and internal sponsor contacts for working with the vendors. Who will you contact about terminating the account?
4. **Written contracts** should outline the rights and responsibilities of all parties. What will you require them to have on their systems? In BAA? Or Separate form for IT?
5. **Ongoing Monitoring.** Password Access Management and Session Recording

NEW 3RD PARTY ASSESSMENT



- Do legal, supply chain, or other departments or leaders include a security assessment review prior to contracts being signed or applications or projects being purchased?

- Is proper due diligence being conducted in selecting a third party by including a security risk assessment?

- A security assessment prior to contract signing allows time for risks and weak controls to be identified and remediated or included in part of contract or the statement of work.

- Establishing a policy and procedure for internal review creates a strong foundation for minimizing vendor and 3rd party risks.

- Communicate the workflow change to include and require a security assessment for any new purchase or contract signing.

WHAT IS HIGH RISK?

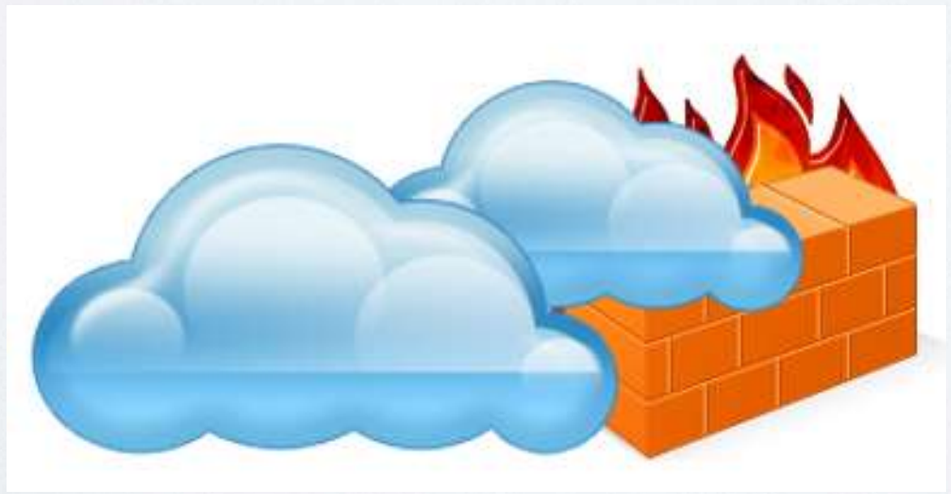
- Identify what high risk controls and red flags to review.

  For example….Do you care if they capture your patients PHI data in their database, shared with other clients, on an unencrypted server, without any intrusion detection or limited firewall protection? What if they don't have any 3rd parties audit their vulnerabilities or have any breach notification procedure or plan? Do you need to pen test their systems? What if they…?

- **Review the findings and require the vendor to correct weak controls to be in compliance and get changes in writing in the contract or statement of work.**

CLOUD RISK MANAGEMENT

- Are there software applications that that your end users are using on the internet? Are you sure you know about all of them and what data is stored?
- How about vendors or contractors that are using AWS cloud services to process your data for their business services? Do you know what they use?



CONTINUOUS….

- ✓ Found all your vendor users? Designated an internal sponsor? Collected contact information?

- ✓ Vendor user access workflow defined? Who approves and reviews?

- ✓ Create risk assessment for identifying high risks and establish a procedure for supply chain and legal to include in the process

- ✓ Identify cloud risks and where extra firewalls and controls are needed and include in contracts and statement of work

- ✓ **Audit to ensure process is working and risks are mitigated**

CYBERSECURITY INFORMATION SHARING

CYBERSECURITY INFORMATION SHARING

- Why is it important?
  - Bad guys are helping each other, shouldn’t we?
  - Automated tools, Dark web
  - Their job is easier than ours

CYBERSECURITY INFORMATION SHARING

- What are the risks?
  - What are we willing to share?
  - Threat information?
    - Known vulnerabilities?
    - Risk assessments?
    - Reputational risks
    - Legal issues
- Security should not be a competitive differentiator

CYBERSECURITY INFORMATION SHARING

- How can we do it?
  - Venues like this, networking.
  - Structured approaches

    Antivirus/security tools provide some level of this – but may be more commercialized

    ISAO – Information sharing and analysis organizations
    https://www.dhs.gov/isao
    ISACs– Information Sharing and Analysis Center

CYBERSECURITY INFORMATION SHARING

- NH-ISAC: https://nhisac.org/
  - Cyberthreat Intel Sharing
  - Daily Threat Alerts
  - Automated Intel Sharing
  - Webinars & Education
  - Regional Workshops
  - Bi-Annual Summits

MEDICAL DEVICE RISK

- Line between IT and Biomed is becoming more and more blurred
  Biomed devices designed using PC architecture

- Biomed devices land as software on IT devices
  - Desktops
  - Laptops
  - Mobile devices
  - Wearable

- Clinical and non-clinical data propagate on the same network
  Clinical and non-clinical data use the same backend storage and other infrastructure

MEDICAL DEVICE RISK

Date	Source	Security Finding
2011	Black Hat Conference	Ability to remotely interfere with the clinical operation of an insulin pump demonstrated
2012	Black Hat Conference	Use of a pacemaker to deliver electrical shock to patient
2013	US GAO	Reported on the above 2 cases and suggested FDA be more involved
2014	TrapX Security	60 hospitals tested to reveal compromised medical devices
2015	FDA	Hospitals notified to stop using Hospira's Symbiq infusion pumps
2015	Bloomberg	"It's Way Too Easy to Hack the Hospital" (Mayo Clinic Research paper)

CYBERSECURITY INFORMATION SECURITY

Md-viper.org

Medical device vulnerability intelligence program for evaluation and response

Goals:

(1) provide a medical device vulnerability sharing, evaluation, and response service;

(2) support FDA’s Postmarket Management of Cybersecurity in Medical Devices final guidance;

(3) create an open community of medical device cybersecurity stakeholders (manufacturers, healthcare delivery organizations (HDOs), independent security researchers, regulatory agencies, etc.) to promote a consensus & consistency of vulnerability reporting and information sharing approach and process;

(4) contribute significantly to medical device cybersecurity education; and

(5) foster situational awareness of medical device cybersecurity threats, best practices and mitigation strategies.

Free to join

ND HIMSS SECURITY PANEL

- Questions/comments?