TECH BELT
Technology Summit

TECH BELT
Technology Summit

How To Avoid a Cyber Attack At Your Business

Top 10 Major Threats of 2014

RECLAMERE
Data Security Experts

The Law & Security

- State Data Breach Notification Laws
- Regulatory / Industry-Specific
  - HIPAA, HITECH
  - GLB, SEC, FACTA
  - FTC
- Commercial Penalties
  - Civil Litigation
  - Negative PR
  - Financial Losses

TECH BELT
Technology Summit

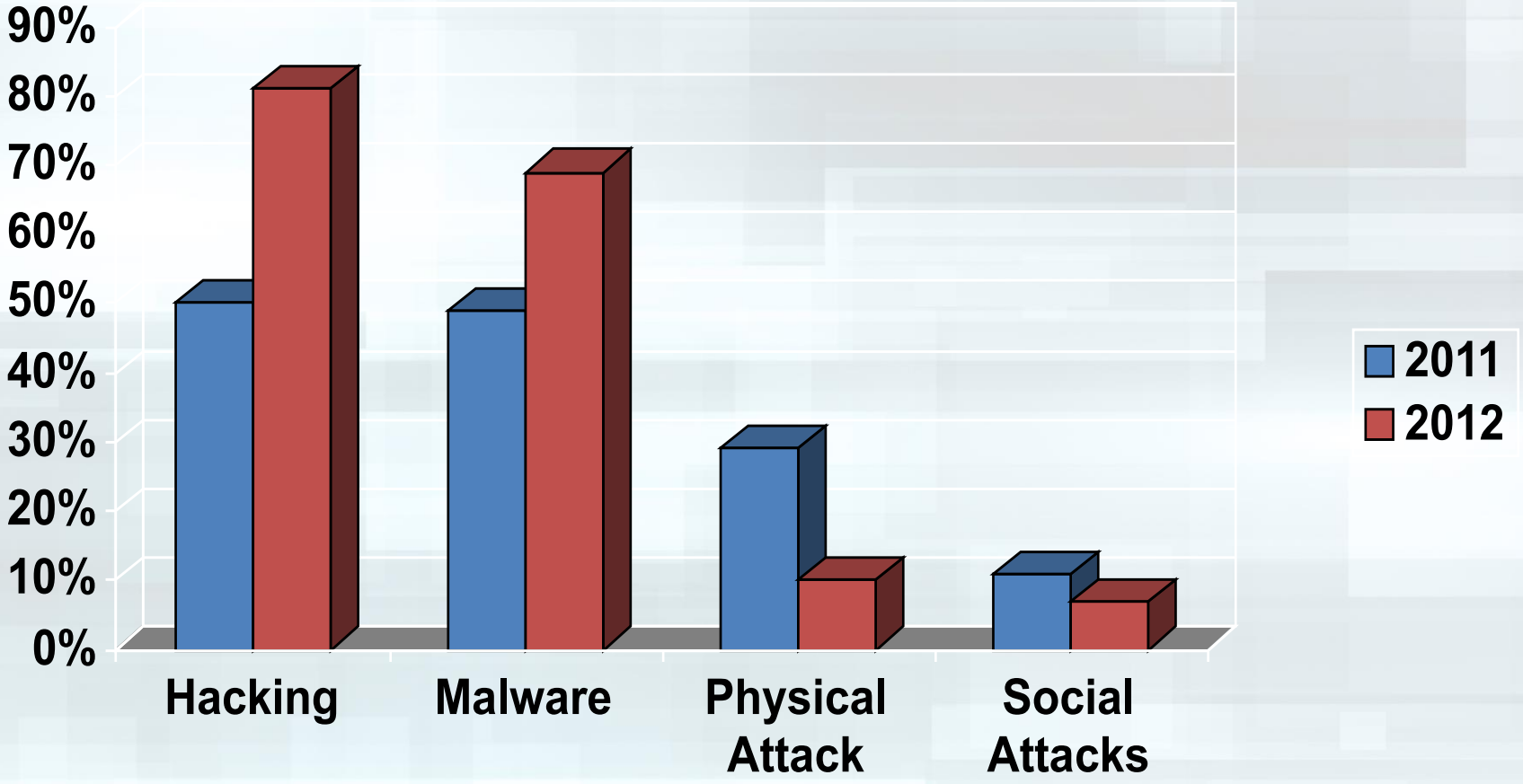
2012 / 2013 Review[1]

- Civil & Cultural Uprising - Hactivism
  - Syrian Electronic Army
  - Anonymous
  - Cyber Fighters of Izz ad-din Al Qassam
- Sophisticated Cyber Crime
  - Financial Losses Targeted at Specific Industries
- Major Data Breaches
  - 855 Incidents, 174 Million Records (2012)

1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

TECH BELT
Technology Summit

How Do Breaches Occur?[1]



1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Breach Commonalities[1]

- 96% of attacks were not difficult
- 85% of breaches took weeks to discover
- 92% of incidents discovered by 3rd party
- 97% of incidents were avoidable with simple or intermediate controls

1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

10. Social Media / Infected Websites

- Hidden Malware (“Like” button, Apps)
- Malicious code embedded in trusted sites (Watering Hole, Hijacked Links, Fake Sites)
- Social Engineering used to profile the browsing habits of target organizations or people
- *Block Social Media sites internally*
- *Train users of dangers and acceptable usage*
- *Update policies to include social media*
- *Keep systems/software/firmware/patched*

9. Smartphone / Tablet Malware

- App Stores with rogue apps
- Text messages that hijack phone numbers and wireless accounts, emails that install keyloggers or other malware
- No platform is inherently good or bad
- *Use security apps / passcodes*
- *Avoid replying to text messages; call until you know the sender is legit*
- *Never click on links in texts from anyone*
- *Encrypt your device!*
- *ALWAYS apply updates to software and devices*

8. Windows XP Retirement

- April 8, 2014 final patches issued
- **Fire "IT guys" that say it won't happen**
- No more patches, service packs, or updates will make systems instantly vulnerable
- Critical Infrastructure? ATM's, Medical Equipment, Financial Systems, SCADA

- *Replace hardware or upgrade Windows*
- *Perform a risk assessment of systems to see what might be running XP "under the hood"*

7. Over-Confidence in AV

- No such thing as “perfect anti-virus”
- Example = annual flu vaccines
- Also beware of fake anti-virus
- Single layered approach
- *Consider managed security monitoring*
- *Require frequent auto signature updates*
- *Train users about fake AV; do not click*

6. Lost or Stolen Devices

- Laptops, Smartphones, USB drives
- Lost backup tapes
- Data breach notification, privacy laws, OCR Wall of Shame, litigation
- *ENCRYPT NOW – No excuses!*
- *Perform vendor due diligence*
- *Include lost/stolen devices in your incident response plan*

5. Content Management Systems (CMS)

- Joomla, Wordpress, Drupal
- Allows user to update websites
- Rarely patched, viewed as “harmless”
- *Do not allow users to install any CMS without permission and a patch management process*
- *Do not allow systems with CMS on same network as sensitive/regulated data*

4. Poor Password Practices

- Same password used for everything
- Passwords never changed
- Simple, easily guessed passwords
- *Use technology to:*
  - *Force strong passwords*
  - *Force regular password changes*
- *Educate users about passwords*

3. Phishing & Spear Phishing

- Disguised links in email
- Social engineering to target specific people
- Uses email, social messaging, or web links
- URL shortening presents new problems
- *Train users on scams continuously*
- *Allow only 1 admin to send out security alerts*
- *Patch systems/AV, control user privileges*

2. Unpatched Machines

- Operating System Patches
  - Local machines AND servers AND gear
- 3rd Party App Patches
  - Office, AV, Obscure Apps
- Old exploits still happening
- *Force justification for patch delays*
- *Enable automatic updates (if possible)*

1. Data Hostage-Taking

- Hackers encrypt all data of organization
- Send a ransom note & “proof of life”
- Demand ransom be paid for encryption keys
- Medical organizations most recently targeted
- Ransom sent through a series of cyber money mules and offshore hacker banking websites

1. Continued

- Loss of data access / billing systems can bankrupt a small business
- *No matter the size of the organization, keep mission critical systems secure*
- *Annual security audits by trusted IT security experts (NOT resellers)*
- *BACKUP, BACKUP, BACKUP!!!!*

Honorable Mentions / Bonus

- HIPAA – Final Omnibus Rule
- Cloud – To Cloud or Not To Cloud…
- Insider Threats
- Civil Liberties / Big Data / Privacy

Small Organization Focus

- Implement Firewalls
- Implement Access Control on remote access services
- Change default credentials on all internet facing devices
- Trust but VERIFY – Minimum annual security testing

Large Organization Focus

- Eliminate unnecessary and / or legacy data
- Monitor logs – outsource / co-source
- Annually review incident response plans – verify with gap analysis
- **Trust but VERIFY – security testing with social engineering, ethical hacking and aggressive penetration testing

TECH BELT
Technology Summit

Questions

Joseph P. Harford, MS, CIPP, CSDS

Founder

814-684-5505 ext. 305

www.reclamere.com

joseph@reclamere.com

RECLAMERE
Data Security Experts

TECH BELT
Technology Summit