Managing IT Risk for Nonprofit Organizations with a Remote Workforce

Aldrich Technology LLP

Peter Adams

VP BUSINESS STRATEGY

PAdams@AldrichTechAdvisors.com

408-884-3690

Aldrich Technology

- Information Security
- Software Solutions
- Merger + Acquisition Support
- Managed IT Services

Productivity or Security?

They are not mutually exclusive…

#1 must be Organizational Productivity

#1.1 must be Risk Management

#2 is everything else…

What is Risk?

Risk is anything that gets in the way of your success or limits your success.

Kinds of Risk:

- Insurable Risks
- Uninsurable Risks
- Knowingly assumed Risks
- Surprise Risks

Continuing Evolution of Cybersecurity

Evolving Threat Landscape

- Last year's cybersecurity thinking is inadequate against this year's threats
- Threats are growing in number, complexity, sophistication, and consequence
- Most IT departments are playing a never-ending game of catch-up – with your organization

ESTĒE LAUDER

What was stolen?

Over 25 Billion Records which include information such as:

- Names, addresses
- Gender, marital status, spouses, and sexual preferences
- Medical history, prescriptions, and formulations
- Account usernames and passwords
- Conversations, email, text, private sites, etc.
- Videoconference sessions
- Security tokens
- Device information
- Miscellaneous user details such as spoken language
- Transcripts of email correspondence
- Payment logs including credit card type, amount paid, and applicable currency
- IP addresses, Trade secrets, National Secrets

What's it Worth?

According to Keeper Security...

Social Security Number	$1.00
Drivers license	$20.00
Credit Card	$8.00 - $22.00
Email Address & Password	$0.70 - $2.30
Medical Record	$1.50 - $10.00
Complete Medical Record	$1,000.00

Ransomware

$50 - Ransomware kits on the Internet

$233,817 – Average ransom demand

25% - Victims pay hackers

30% - Average amount of data recovered after paying ransom

$20B – Ransomware cost to business in 2020 ($11B in 2019)

2020 Targeted Organizations

- 113 Government agencies
- 560 Healthcare facilities
- 1,681 Schools were impacted

Consequences

Would these consequences impact your ability to:

- Operate?
- Pay your Employees?
- Serve your Constituents?
- Fulfill your Mission?

How Do I Protect My Organization?

- Establish IT Governance
- Experience and Accomplishment
- Rely on competence rather than on personality/tenure/relations
- Develop an IT Strategy
- Pay attention to the Details
- Execution and Verification

Standards Bodies

National Institute on Standards in Technology (NIST)

Cybersecurity Maturity Model Certification (CMMC)

Payment Card Industry (PCI)

* Leverage standards – don't make it up on your own!

Components of Security

- People and their Practices
- Technologies
- IT Policies
- Incident Response

Helping People with Security Practices

- Education
- Recognize threats like spam, phishing, spear phishing
- Create people-centric controls
- Create people-centric IT Policy
- Passwords and Passphrases
- Two-Factor Authentication
- Establish Roles & Responsibilities
- Access Controls based on Roles (does everyone need access to everything?)

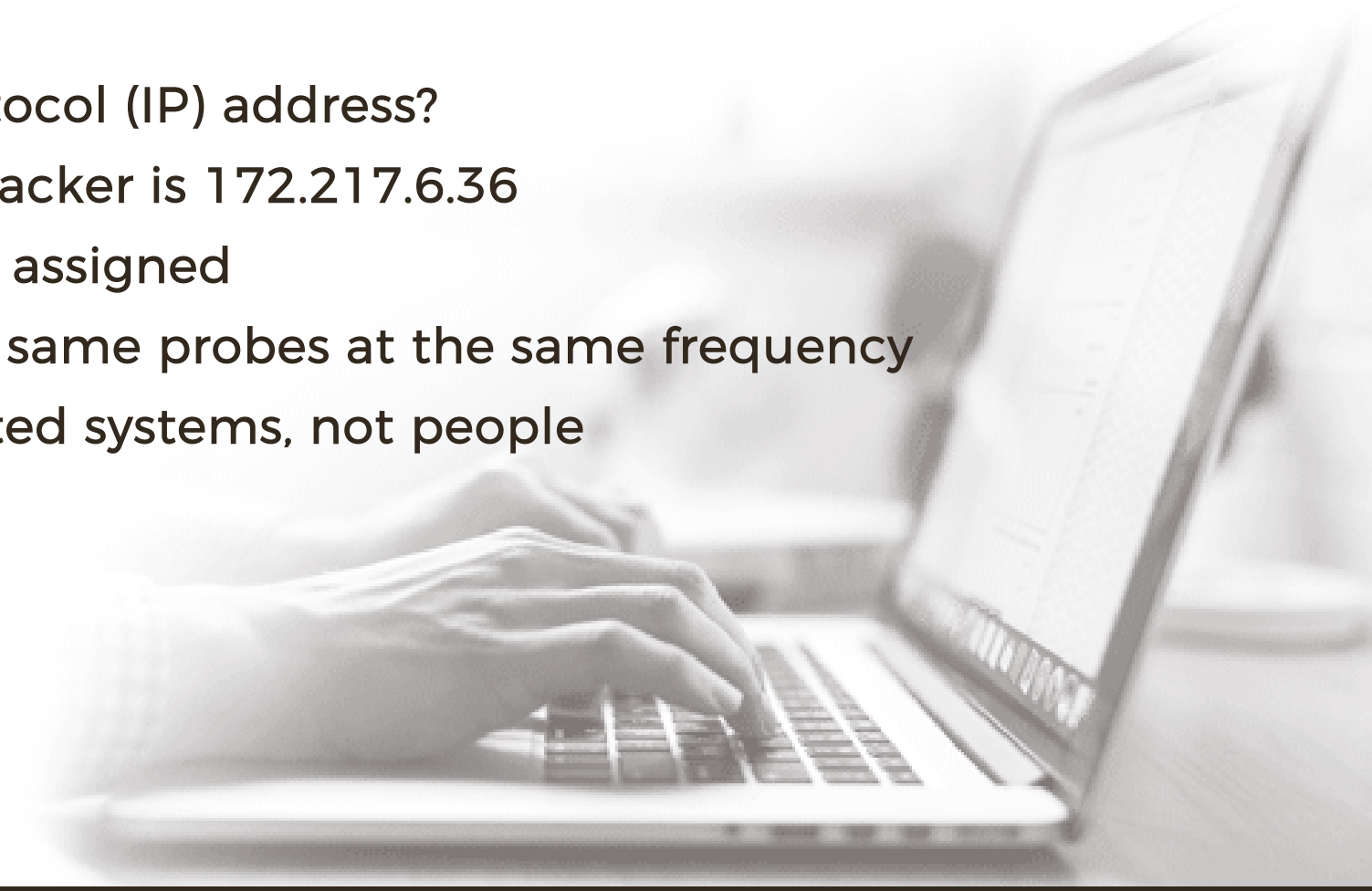
Who are you in the world?

Who Are You?

You are an address.

- What is an internet Protocol (IP) address?
- www.google.com to a hacker is 172.217.6.36
- IP addresses are usually assigned
- All IP addresses get the same probes at the same frequency
- This is done by automated systems, not people

It is not personal.



How long does it take to crack your password?

“bankers”	7 characters	.29 milliseconds
“b@n4er$”	7 characters	.29 milliseconds
“football”	8 characters	5 hours
“F@@tballz”	9 characters	5 days
“Metrology$”	10 characters	4 months
“FlowMatters”	11 characters	1 decade

Security Through Architecture

Aldrich

What to do about cell phones???

Organization
Users

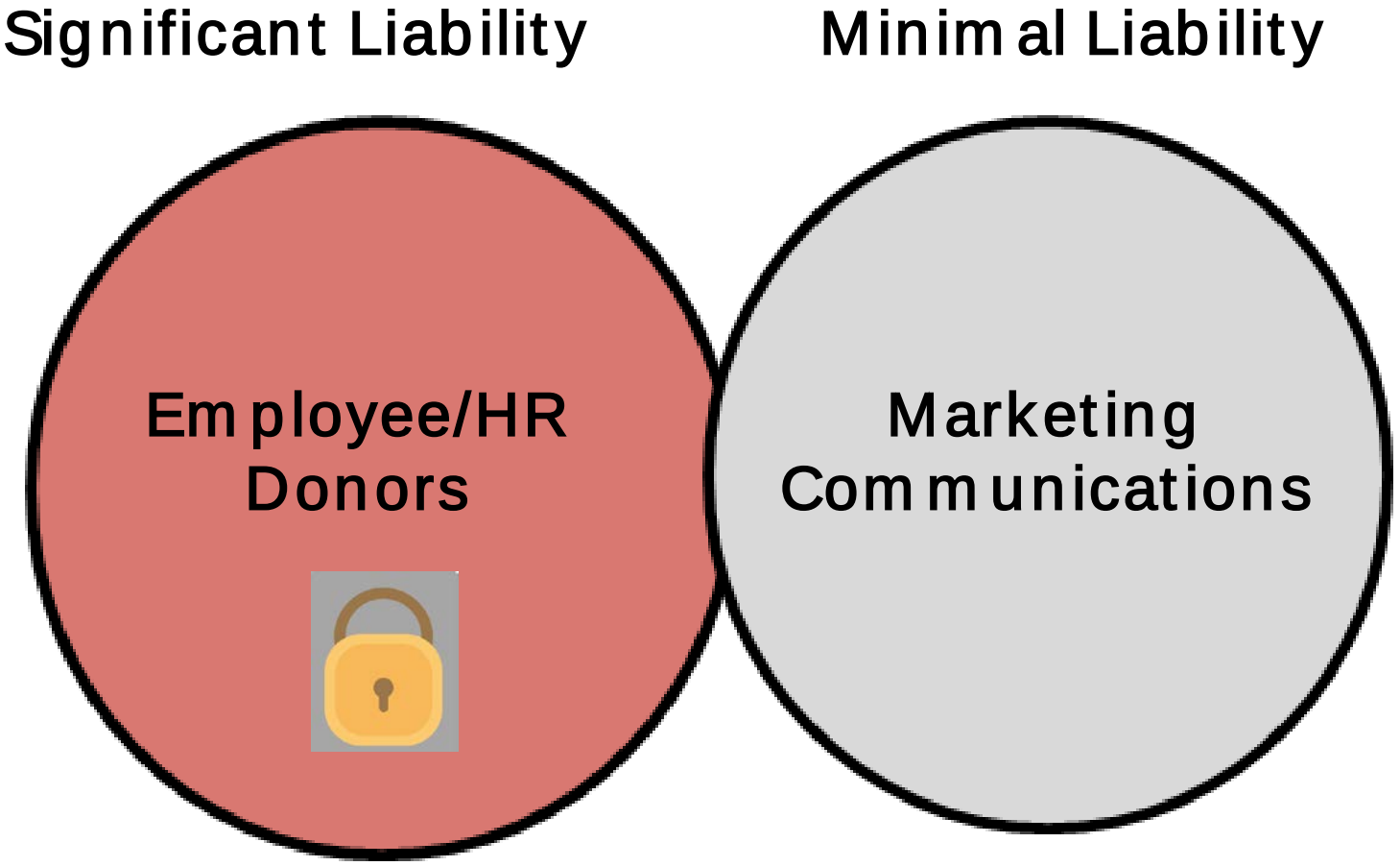
Internal Secure Network

Guests
Cell Phones
Tablets

Internet ONLY

Aldrich

Is all data equal???



Good Technology Security Practices

- Maintenance, Administration & Patching
- Maintaining software at current/supported release levels
- Remove old accounts
- Anti-Spam and Anti-Virus
- Firewalls
- BotNet Filters
- Backups
- Encrypt laptop data
- Cell/smartphones
- Wireless Network Authentication (no Pre-Shared Keys!)

Good Security Policies

Leverage Policies to enforce what is and is not permitted

- Written Policies
  - Employee Handbook
  - Technology Usage
  - Code of Conduct
- IT Policies
  - Password Policy
  - VPN Policy
  - Application Policy
  - Cell/Smartphone Policy

Good Security Response

- Develop an Incident Response Plan – simple or complex
- Monitoring is not the answer alone, it is a piece of the answer
- People need to let IT know when they suspect something unusual or weird
- IT needs to take PROACTIVE action to:
  - Educate people
  - Maintain the network to always current
  - Be diligent about administration
  - Respond quickly and appropriately to the ever-changing threats
  - Educate people
  - And Educate people

Case Studies

Security vs Productivity

- Nonprofit with extreme security
- Employees not able to work effectively
- Current infrastructure inhibiting ability to accomplish their mission

Case Studies

IT Governance

- Nonprofit with no IT Governance
- Each department chose own software applications
- No consideration of the entire organization
- No master data shared across systems to evaluate programs, donors, etc.

Case Studies

Weak security policies

- Password policy not enforced
- No Multifactor Authentication
- Employee's email hacked

Important Take-Aways

- Boards have a fiduciary responsibility to ensure their organizations are taking appropriate documentable/verifiable actions to mitigate cyber risks.
- Cyber Insurance only covers insurable risk. Uninsurable risk is still significant
- Establish sound IT Governance
- Bring in competence where needed

Peter Adams

VP BUSINESS STRATEGY

PAdams@AldrichTechAdvisors.com

408-884-3690

Aldrich Technology

- Information Security
- Software Solutions
- Merger + Acquisition Support
- Managed IT Services