Take Risks in Life, Not with Your Security

Redefining Cybersecurity
Agenda

• Current Threat Landscape
• People are the Problem
  – Protect Yourself
• Solutions for the Organization:
  – 360° Security
  – Security Policy
  – Incident Response
  – Security Awareness Training
  – Brilliance in the Basics
Why We’re Here
The Problem(s): Threat Landscape

**SOCIAL ENGINEERING**

95% of all attacks on enterprise networks are the result of successful spear phishing.¹ 233% increase in phishing URLs from 2013 to 2014.²

**MALWARE**

159% increase in malware URLs
50% increase in average daily number of malware emails
61% increase in mobile malware³

**INTERNAL USERS**

35% of all data breaches globally concerned a negligent employee or contractor.³

**RANSOMWARE**

CryptoLocker

**MALICIOUS PAYLOADS**

**APT (Advanced Persistent Threat)**

**ZERO DAY ATTACK**

---

It’s Getting Worse

OVER THE LAST 4 YEARS

The number of successful cyber attacks on businesses increased by 144%.

The cost of cyber crime per company has increased by 95%.

The average time to resolve incidents has increased by 221%.

95% of all attacks on enterprise networks are the result of successful spear phishing.  

---

Why the Bad Guys are Winning

2015 Focus

60% of the time attackers get into a firm within minutes.

75% of attacks spread from victim to victim within 24 hours.

Deploying just 10 phishing emails yields a greater than 90% chance that at least one person will click.

99.9% of vulnerabilities exploited are actually a year old.

Source: 2015 Verizon Data Breach Incident Report (DBIR)
Why It Matters

WHAT'S YOUR RISK?

$5.4M + Average cost of a data breach in the U.S.¹

$3M Average cost of lost business a U.S. firm experiences after a data breach¹

Financial Risk
Operational Risk
Reputational Risk

¹ Source: 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute
The New Normal

There are only two types of companies – those that have been hacked, and those that will be.

- Robert Mueller, Former FBI Director

There is no finish line when it comes to cybersecurity, and it needs to be everyone’s #1 agenda.

- Marc Benioff, CEO of Salesforce.com

It’s only a matter of the ‘when,’ not the ‘if,’ that we are going to see something dramatic.

- Admiral Michael Rogers, Director of the National Security Agency
People are the Problem

The common denominator among the top security patterns - accounting for nearly 90% of all security incidents - is people.

- 2015 Verizon Report
#1 Killer: Phishing

<table>
<thead>
<tr>
<th>Company</th>
<th>Type of Breach</th>
<th>People Affected</th>
<th>Cost/Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>SONY</td>
<td>Spear Phishing</td>
<td>UNKNOWN</td>
<td>COST UP TO $300,000,000</td>
</tr>
<tr>
<td>ebay</td>
<td>Phishing Scam</td>
<td>145 MILLION</td>
<td>COST UNKNOWN</td>
</tr>
<tr>
<td>TARGET</td>
<td>Phishing Scam</td>
<td>110 MILLION</td>
<td>COST $61,000,000</td>
</tr>
<tr>
<td>THE HOME DEPOT</td>
<td>Phishing Scam</td>
<td>56 MILLION</td>
<td>COST UP TO $62,000,000</td>
</tr>
</tbody>
</table>

- **AGIO**
How many of you, or your employees, use the same password for personal accounts as you do for your firm’s systems?
Be Proactive

🔑 Use separate passwords for firm/personal use. Use a strong password or other user authentication (PIN protection at a minimum); change often.
   a. Consider using a password management tool (LastPass, KeePass, or Password Safe).

🏠 Do not exchange home and office content.

✉️ Do not click on email or pop-up messages asking for personal or financial information.
   a. Caution: “Reply link/button” or “unsubscribe link/button.”
   b. Hover over links to determine the destination URL.

💰 Never email personal or financial information.

⚠️ Be cautious when opening attachments or downloading files from emails you receive.
Be Cautious on Social

Facebook, Twitter, Instagram, etc.

1. Know what others can see on your profile

2. Control who can tag you in photos

3. Secure login and account reset

4. Limit public availability of location data (i.e. when you’re on vacation)

5. Review activity logs
Mobile Devices

1. Privacy Settings
2. Encryption
3. Remote Wiping
4. Secure Wi-Fi
7 Deadly Sins

1. Unnecessary Administrative Account Use
2. Software Downloads from Untrusted Sources
3. Inconsistent Use or Lack of Anti-Virus
4. Inadequate Monitoring of Financial Account Activity
5. Surfing Risky Sites (gambling, foreign, etc.) – Malvertising
7. Clicking Before You Think
Solutions for the Organization
Agio’s security philosophy is founded on and executed through our diligence, expertise, process and technology. We protect your environment 24x7x365, from the inside out.
Start with a Security Policy

1. Executive Buy-In: This is a Business Problem

2. Where’s Your Sensitive Data?
   i. Create Inventory (Data Map)
   ii. Protect Based on Level of Risk, Budgetary Constraints, etc.

3. Determine Risk. Understand:
   i. Weaknesses (End of Life Software, Public Facing Servers, etc.)
   ii. Potential Exploits (Heartbleed, Shellshock, GHOST, etc.)
   iii. Probability

4. Establish Regular Schedule of Reviews & Updates
   i. Constantly Evolving Threat Landscape

5. Protect Network's Physical Security. Physical Access To:
   i. Computers
   ii. Routers
   iii. Firewalls
Master Your Incident Response

1. Understand Threats to Your Firm

2. Establish Roles & Responsibilities for Response
   i. Internal v. External Resources
   ii. Train Internal Staff Related to Assigned Roles

3. Understand Legal Landscape & Document Applicable Requirements
   i. Include in Policies & Procedures

4. Contractually Require Vendors to Notify You When they Experience a Breach
   i. DDQ
   ii. Control Validation

5. Tabletop Exercises
   i. Test Validity of Plan
   ii. What’s the Chain Reaction?

6. Engage Legal Council & Your C-Suite Colleagues
Fortify Your Weakest Link

Technology Doesn’t Secure Your Environment; People Do.

Employees & Contractors are Given Access to:
- Computers on the Network
- Gates
- Locked Doors
- Authentication Systems
- Firewalls & Encryption Systems

Security Awareness Training:
- Seminars
- Computer-Based Training:
  - Real-World Examples
  - Malware
  - How to Define a Security Incident
  - Reporting of Anomalous Activity
Brilliance in the Basics

- System Hardening (configuration defaults, etc.)
- Enable Two-Factor Authentication
- Enforce Strong Passwords
- Apply Principle of Least Privilege Use
- Install End-Point Protection
- Implement Network Segmentation
- Perform System Maintenance (Patching)
- Install Security Identification & Event Detection
- Monitor Anomalies (Active Anomaly Detection)
- Test
- Conduct Security Awareness Training
Questions?