Expanding your Blue Team by Creating Security Culture

Masha Sedova
Co-Founder, Elevate Security
@modMasha
masha@ElevateSecurity.io
About Me

• Background in security with a love of positive psychology, human motivation, and behavioral economics.
• Built and ran Salesforce’s Trust Engagement team for 5 years.
  • Ran a team responsible for general employee security culture, secure development and engineering practices, and customer security advocacy.
• Started Elevate Security in late 2016 to focus on behavioral science based security awareness.
• Passionate about transforming security behaviors from “have to” to “want to” by looking at the full scope of an employee’s experience.
CISOs’ Top Two Threats in 2015
Percentage of CISOs who believe this poses a high or existential threat

- 61% Unauthorized Use of Employee Credentials
- 72% Spearphishing

Employees a Key Cause of Breaches
Percentage of CISOs who believe insecure employee behaviors lead to breaches

- 50% of CISOs believe over half of breaches are a result of insecure behaviors.

Source: CEB 2014 Threat Landscape Survey
Source: CEB March 2015 Information Risk Peer Perspective Survey.
Employees Are Sources of Information About Risks and Breaches

Percentage of CISOs

- 9% Somewhat Disagree/Disagree/Strongly Disagree
- 4% Neutral
- 23% Somewhat Agree
- 32% Agree
- 32% Strongly Agree

$n = 89.$

Source CEB March 2015 Information Risk Peer Perspective Survey.

Employees as Breach Detectors

2014 Verizon Data Breach Report

“...over the years we’ve done this research, users have discovered more breaches than any other internal process or technology. It’s not all about prevention; arm them with the knowledge and skills they need to recognize and report potential incidents quickly.”

Historically, we haven’t given end users much credit
People Centric Security

ˈpēpəl/ ˈsentrik/ si-ˈkyûr-ə-tē/
noun

**Definition:**
Making people central to solving problems rather than contributing to them.

Security teams can give employees the resources to do this better.
Let’s Define Phishing

Phishing

Credential Stealing
- Requires human vulnerability
- Requires unpatched system

Running Malicious Executable
- Requires human vulnerability

Clicking on a link
- Requires human vulnerability
- Requires vulnerability in your browser (i.e., Flash)
Current Best Practices

Goal: Reduce the number of people who click on links
The Problem With Measuring Click Through

- Are your employees smarter or is the test easier?
- Repeat tests can give employees advanced warning.
- What click through rate is good enough?
- When will you be “done” training your employees?
Spoiler Alert: Click rate will never be 0%

- Campaigns with 3 emails give you a better than 50% chance at getting a click
- Sending 10 phishing emails approaches a near guarantee for a click

Source: DBIR 2013
Now What?!

Plan for failure—someone will click
What Happens When an Employee Clicks?

1. They Have No Idea
2. They Don’t Care
   - Take Corrective Actions

In roughly 636,000 sanctioned phishing emails, we captured whether the email was reported. Approximately 3% of targeted individuals alerted management of a possible phishing email.

-DBIR 2016
Impact of clicking (Option #1 or #2)

- Undetected compromised computer
- Rely on downstream mitigating controls (patched systems, antivirus, 2fa, etc) to block malware or prevent password use
- Incident response team is waiting on technical signals (IDS) to alert them of an anomaly, giving the attack a head start (dwell time)
Option #3: Taking Corrective Action

- Train employees to report phishing emails—clicked or not
- Reporting can identify malicious activities not caught by our technology stack.
- Even if an employee is unsure, train them to check with the security team.
- Most employees aren’t security experts. Train employees to leverage security team’s expertise by asking for help.
The Benefits of Reporting

- If a legitimate attack is reported, the IR team can:
  - Quarantine the link and outbound traffic
  - Filter the malicious email from other inboxes
  - Scan for instances of the malware on the network
  - Initiated remediation efforts on potentially compromised computers.

- Encourage reporting even if the end-user knows it’s phishing and does not click on this link.
  - This can block the attack for another employee who isn’t as security aware and clicks the link.

- One person can save the whole company!
What is Success?

20%
Leveling the Odds Against Attackers
How to Maximize Reporting
Is It Safe To Fail?

Image source: http://imgur.com/Yilpfz
Relationship to Failure

VS.

INTERNAL
REVENUE
SERVICE
Potential Impact of Negative Reputation

Not safe to admit failure

“I think I clicked on something that I shouldn’t have.”

Limited proactive, voluntary interactions

“This file looks weird. Can you help me check it out?”

Key issues were not reported for fear of retribution or responsibility

“I’ve noticed this insecure process handling critical data.”

Limited receptivity to key messages

“Security sends me interesting and relevant information that I should be concerned about.”
5 Positive to 1 Negative Ratio
How to Motivate Reporting

- Gamification and point systems
- Leaderboards
- T-shirts, Hats, Stickers (Swag)
- Company wide announcements with recognition
- Thank you emails
Reward: Security Champion Program

- **Apprentice**: Basic awareness
- **Novice**: Successful Testing
- **Knight**: Doing
- **Master**: Teaching
- **Grand Master**: Innovating

Trust Points:
- 100
- 200
- 300
- 400
- 500
- 600
Impact on the Incident Response Team

Salesforce Case Study:

- Increased the volume of emails to the incident response team by 350% in 6 months
- Way more false positives
- Employees over-report emails including poorly formed internal emails, surveys, etc.

This was a business choice that was made.

- Invested in scaling the IR team and automation.
- Automation solutions include auto responding to emails that match previously submitted cases or known phishing tests
Incident Detection Results

- Salesforce employees trained to report *any* suspicious activity
- Customer reports also welcome

“My browser proxy settings were changed.”

“Someone just badge surfed in our main floor.”

“I lost my sweater on the subway.”

“My mouse cursor is moving by itself.”

“Is this email really from American Express?”
Apply It!

Tomorrow:
• Start communicating to employees how to report and why it's important.
• Measure phishing reporting rates in addition to clickthrough rates.

Soon:
• Build a positive relationship with your employees and users early, before you need them to report!
• Use positive reinforcement to drive safety in failure.

Long-term Lessons:
• People are the missing part of the security solution. Convert your largest target into Human Intrusion Detection Systems!
• Enabling your employees to “want to do security” is the next level of maturity for your awareness program.
Questions?

Let’s stay in touch!
@modMasha
Masha@elevatesecurity.io