building a security culture to counter emerging cybersecurity threats
Security Culture

Board of Directors
Executive Management

CSO
CISO

Chuck Kesler

Clyde Hewitt

VP
Directors /Managers
Staff
a security program is only as good as its weakest link, and that link is always the human
our people are both threats and targets

Source: 2017 Verizon Data Breach Investigations Report
email remains a primary threat vector
80% of all healthcare breaches in 2016 had a human component

- privilege misuse
- errors
- physical loss and theft

Source: 2017 Verizon Data Breach Investigations Report
One in five employees are willing to sell their passwords!

<table>
<thead>
<tr>
<th>Country</th>
<th>Proportion of all respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>27%</td>
</tr>
<tr>
<td>Global</td>
<td>20%</td>
</tr>
<tr>
<td>Germany</td>
<td>20%</td>
</tr>
<tr>
<td>UK</td>
<td>16%</td>
</tr>
<tr>
<td>France</td>
<td>16%</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>12%</td>
</tr>
<tr>
<td>Australia</td>
<td>12%</td>
</tr>
</tbody>
</table>

Source: https://qz.com/649996/one-in-five-employees-would-sell-their-work-passwords-some-for-less-than-100/

Data: Sailpoint 2016 Market Pulse Survey
One in five employees are willing to sell their passwords!

<table>
<thead>
<tr>
<th>Country</th>
<th>Average Offer Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>$1,822</td>
</tr>
<tr>
<td>UK</td>
<td>3,874</td>
</tr>
<tr>
<td>Australia</td>
<td>6,478</td>
</tr>
<tr>
<td>US</td>
<td>50,770</td>
</tr>
<tr>
<td>Global</td>
<td>82,507</td>
</tr>
<tr>
<td>Germany</td>
<td>257,775</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>466,667</td>
</tr>
</tbody>
</table>

of the 1,000 survey respondents, the lowest offer accepted was $55

Source: https://qz.com/649996/one-in-five-employees-would-sell-their-work-passwords-some-for-less-than-100/
changing behaviors requires changing culture
levers for creating a strong security culture

• engagement
• leadership
• awareness
• trust
which method works best for engaging employees?
Five critical success factors for employee engagement:

- Effective and consistent leadership
- Goals and objectives that are well understood and supported
- Work/life balance
- Positive organizational image
- Respectful, clear, and encouraging management communications

These factors must be considered when establishing a strong security culture.

Source: Towers Watson Global Workforce Study, August 2014
security culture starts with the tone from the top

- program must have visible executive support
- solicit and incorporate feedback from board and operational leaders
- make sure they are committed to walking the walk, not just talking the talk
- enlist their support for communications
we’re working hard to get the message out

• online training modules
• newsletters
• email blasts
• posters
• presentations
• simulated phishing
• sanctions
so why doesn’t the message stick?

- complex
- confusing
- corporate
- infrequent
- inconvenient
- reactive
- FUD
security awareness isn’t enough
to change our culture, we need a new state of mind
mindfulness

mīn(d)f(ə)lnəs

noun

1. the quality or state of being conscious or aware of something
2. a mental state achieved by focusing one's awareness on the present moment
security

mindfulness

səˈkjʊrəti mîn(d)f(ə)lnəs

noun

1. the quality or state of being conscious or aware of security threats and best practices
2. a mental state achieved by focusing one's awareness on potential security threats in the present moment
creating security mindfulness through better messaging

- simple
- tailored
- personal
- frequent
- quick
- consistent
- measurable
1. Understand and follow Duke’s security policies.
2. Use strong passwords, and, whenever possible, use multi-factor authentication.
3. Think before I click on links and email attachments.
4. Use a VPN when connecting from public WiFi networks.
5. Apply all security updates in a timely fashion when prompted.
6. Safeguard my personal computers and devices with anti-virus software.
7. Secure my smartphone and computer screensaver with a PIN or password.
8. Use encryption to protect sensitive data when appropriate.
9. Report suspected security concerns immediately to security@duke.edu.
more ideas for creating security mindfulness

• daily reminders delivered via banner messages
• gamification (e.g. contests, simulations)
• no annual training, just an annual quiz
• study the effectiveness of different techniques across your workforce, and tailor future campaigns based on demographics
it takes a village to change culture

• identify individuals who can be ambassadors
• train them on security basics
• advertise them as local experts
• encourage them to spread the word
• recognize their efforts
• rinse and repeat

Example: Duke’s IT Security Academy
trust is a two way street

- employees are concerned about their privacy
- employers should respect that privacy
- transparency around monitoring is critical
- policies should set bounds on monitoring
- IT and security staff must operate ethically
- those breaking this trust must be held accountable

Example: Duke’s Acceptable Use Policy
People remain the biggest security asset
Defining a Culture of Cybersecurity

• Cybersecurity is a management problem, not a technology problem

• People continue to be the biggest security threat, but also a security asset
  – Protecting all sensitive information is everyone’s job

• A strong cybersecurity culture in ubiquitous to business operations
  – Not derived from a mandate to follow a specified path from IT
  – It is everyone’s responsibility to protect systems & data
Characteristics of Good Security Culture

• Executives must talk the talk, but must also walk the walk

• Leadership has set clear expectations that everyone can report suspected security & privacy incidents
  – Anonymous reporting channels are available without retribution
  – No one is exempt from following the rules
Strong Security Culture Demystified

• There is a recognition that patient safety and privacy are critical elements to providing the best care
  – For managers, security culture is demonstrated by their willingness to investigate every reported risk, quickly escalate validated risk to the appropriate level of decision authority, and to act to reduce the risk to an acceptable level as defined by the *published risk appetite*
Cybersecurity Culture Starts in the C-Suite

• Building a governance model where the C-Suite is actively engaged in all cybersecurity discussions
  – Avoid delegating enterprise responsibility

• Set high goals, and measure progress, provide resources
  – Ensure that realistic measurable objectives are defined
  – Do not chase technology, but invest resources on programs that work
  – Be visible at training events

• Stay connected, ask tough questions, expect results
Building the Security Culture

• Everyone from the Board, down through the C-Suite to the individual contributors understands that security and privacy is important
  – The Board should expect frequent updates with measurable security and privacy objectives

• The C-Suite should hold everyone accountable to manage the risks assigned to them, and provide resources when needed

• Finally, the security and privacy compliance team is not limited by a myopic view and evaluates the impact of all operations
Leadership of the Risk Management Process

• The risk management process is the foundation of all security decisions
  – Aligned with the Board’s stated risk appetite
  – Risk analysis determines future investment decisions
  – Risk assessments should be completed just prior to the budget cycle

• Define risk treatment options
  – Importance of using defined terms
  – Aligning responsibility with decision making authority
Questions Executive Leadership Should Ask Themselves

• Are strategic decisions made at the appropriate level in the organization
  – Designed to address all security requirements
• Do we have a formal governance structure
• Have we adopted a security framework
• Have we aligned with the organization’s processes
• Do we support the principle of continuous improvement
Board of Directors Role

- Recognize that cybersecurity is an enterprise-wide risk management problem
- Understand the legal, regulatory, & contractual cybersecurity obligations
- Ensure access to cybersecurity expertise
- Grant adequate time on Board agenda to discuss cybersecurity issues
- Set clear expectations that cyber risks management framework is required
- Understand details of the cyber risk management & treatment program
Questions Board Members Should Ask Themselves

• Do we have the right talent leading our security, privacy, & compliance teams
  – Have we established clear objectives to guide them
  – Do we get other views to avoid ‘rose-colored’ glasses

• Are there clear lines of responsibility / authority
  – Have we clearly communicated that to everyone

• Are we communicating importance of cybersecurity to the workforce
  – Do we hold people accountable
  – Have we set an acceptable level of risk appetite
Cybersecurity Disclosure Act of 2017

• The Cybersecurity Disclosure Act of 2017 (S. 536), introduced March 7, 2017 by Sens. Mark Warner (D-Va.), Jack Reed (D-R.I.), and Susan Collins (R-Maine), also would require companies that don’t have a cybersecurity expert on their boards to explain in financial filings why they considered the expertise unnecessary.

• Applies to publically traded companies

• Monitor progress as this moves through Congress
7 Elements of an Effective Compliance Program

- Conducting internal auditing & monitoring
- Implementing compliance & practice standards
- Designating a compliance officer or contact
- Conducting appropriate training and education
- Responding appropriately to detected offenses & developing corrective action
- Developing open lines of communication
- Enforcing disciplinary standards through well-publicized guidelines
Strengthening Processes

Governance
Security Management
Risk Management
Vulnerability Management
Access Management
Activity Monitoring
Incident Response
Supply Chain Security
Strengthening Relationships

“The supply chain provides a necessary and critical component of care delivery today”

• Healthy third-party relationships start with due diligence
• Smart healthcare organizations partner for success with security vendors
• Partners fill gaps in expertise, information, industry knowledge, etc.
• Ensure objectivity and due diligence in evaluations
Q&A

Clyde Hewitt
Vice President of Security Strategy
CynergisTek, Inc.
clyde.hewitt@cynergistek.com
Twitter: @cynergistek

Chuck Kesler, MBA, CISSP, CISM
Chief Information Security Officer
Duke Health
chuck.kesler@duke.edu
Twitter: @chuck_kesler