THE HUMAN ELEMENT OF DATA PROTECTION

JEFFREY E. LEWIS

IT'S ALL ABOUT PEOPLE.

HUMAN ELEMENT OF DATA PROTECTION

- Effectively protecting sensitive data has evolved to move beyond building technical walls to protect data.
- The more omnimous threat is caused by the exponentially increasing amount of data access that is granted to insiders, some—not all-- of these insiders with malicious intent to use of data.
- As data warehousing, hosting, and retention has moved from mainframes, more data is held on personal devices and laptops and sometimes that data is transmitted through unsecured means such as WiFi.

HUMAN ELEMENT OF DATA PROTECTION

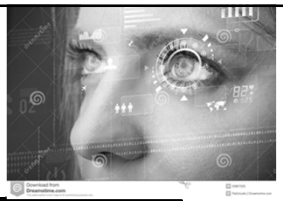
People cause breaches. Examples of non-malicious causes include:

- Social engineering
- Leaving devices unattended.
- Sharing passwords
- Entering passwords into spoofed websites.
- Downloading apps or opening email attachments with embedded malware.
- Parking sensitive data in cloud/internet locations for later use.
- Emailing sensitive information unintentionally or to non-trustworthy recipients.

HUMAN ELEMENT OF DATA PROTECTION

- Studies have shown that almost 80% of organizations, large and small, have experienced some form of data breach as a result of improper or malicious employees or third parties.
- While cyber threats continue to pose risks, the overwhelming majority of data breaches are not caused by external cyber attacks.
- Internal causes of breaches run the gamut of loss of laptops or devices, malicious employees or insiders, carelessness, and social engineering.
- Most organizations still point to employee negligence as the top threat to information security.

HUMAN ELEMENT OF DATA PROTECTION



- Technology is increasingly being used to detect breaches caused by human factors.
- Typically, breaches are discovered through internal audits and investigation, mere accidental discovery, complaints by consumers or victims, self-reporting by employees, and technology.
- Technology is key in detecting breaches and improper access. Technology includes detection of anomalous behavior, tracking access to sensitive data; limiting transmission of data outside of internal systems, etc.

HUMAN ELEMENT OF DATA PROTECTION

Emerging consensus on ways to protect sensitive information from data breaches. These include:

- Security/breach detection technology.
- Access governance-least privileged access doctrine.
- Consistent training and employee education.
- Multi-factor authentication.
- Physical security and limited physical access.
- Employee awareness that breaches harm the enterprise and could impact job security.
- Limiting what websites employees can access; limit what types of emails can be sent; setting triggers and alerts when sensitive data is transmitted via email.

HUMAN ELEMENT OF DATA PROTECTION

Best practices:

- Develop a comprehensive information security program, with input from business operations, IT, audit, legal, regulatory, compliance, finance, and chief security office.
- Get third-party vendors involved in training and data protection awareness. Encourage or require vendors to implement comprehensive data security processes.
- Establish a data security, cross functional, working team, with support from highest levels of organization.
- Set priorities for highest level of protection for the most sensitive individually identifiable personal data.
- Establish written policies for data protection.
- Limit sensitive data that employees can carry on their laptops, iPads, and mobile devices. Massive amount of digital information available on devices can expose millions to harm. (Example: laptop stolen from back seat of car.)
- Repeat---limiting privilege and access to data is key. What data elements are actually needed by the employee to do their jobs? Does employee need access to social security, credit card, drivers license, DOB information in order to provide particular services? Does employee need access to data when switching roles or departments?

HUMAN ELEMENT OF DATA PROTECTION

Training is key.

- Training should be easy to understand and relevant to the particular audience.
- Debate: should employees be told that their actions are being monitored?
- Make training fun and relevant. Consider monthly reminders in newsletters and break-out sessions.
- New employees should be trained before granted access to data and incumbent employees should be trained periodically (at least on an annual basis, with periodic refresher training).
- Employees should be encouraged to speak up..”say something if you see something”.
- Educate employees on the fact that breaches are not always caused by malicious actors. Most breaches occur through carelessness or failing to follow prescribed processes.
- Educate employees on new and emerging data breach schemes.

HUMAN ELEMENT OF DATA PROTECTION

- Social engineering is a serious threat. Don't ignore the fact that bad actors use social engineering schemes to improperly obtain sensitive data.
- Understand that employees are under pressure to help customers-–and do so as quickly as possible. There may be unintentional inducements for employees to "cut data security corners", i.e., aggressive sales targets. .
- Encourage employees to think holistically; attend hackathons; being observant and aware is "good cyber hygiene".
- Important that employees understand the "why" of data protection and the consequences of security breaches, including fines by federal or state regulators, losses by the company, loss of jobs by employees, and reputational risk to the organization. (Example, HR and Finance can outline how data breaches impact the bottom line).

HUMAN ELEMENT OF DATA PROTECTION

Broader trends:

- Increased Board oversight of cybersecurity. Cybersecurity continues to be front and center of board agendas.
- According to a recent PWC report (Global State of Information Security Survey 2018), 44% of executives surveyed say that they don't have information security strategy in place and 48% have not established an employee security awareness program.

Micro trends:

- Limiting use of passwords based on employees' name, date of birth, address, or even childrens' names.
- Increasing use of biometric authentication, via thumbprint or derived credintials from card on phones.

HUMAN ELEMENT OF DATA PROTECTION

Finally……..

- Ensure that your organization has a comprehensive, cross functional, incident response team to timely (i) report breaches to regulators and customers when required by law; and (ii) develop a remediation plan to ensure that similar types of breaches do not occur again.
- Include a cross-functional team of "people" so that all functional areas of the organization are aware of the consequences of breaches.

HUMAN ELEMENTS OF DATA PROTECTION

References include:

- *Cisco tackling human element of security with cyber training course*, Asha McLean, zd.net.com, June 23, 2017
- *Train Your Employees to Think Like Hackers*, Martin Mickos, Harvard Business Review (hbr.org), December 15, 2017
- *The Human Element of Cybersecurity*, Mav Turner, securitymagazine.com, May 26, 2015
- *The Human Factor in Data Protection*, Ponemon Institute LLC., ponemon.org, January 2012
- *The Biggest Threat to Data Security? Humans, of Course.* Richard Kam, app.org, October 22, 2015
- *The Human Factor: Cybersecurity's Forgotten Conversation*, George Plastis, , tripwire.com, April 19, 2017
- *Insider Threats: Tackling the Human Element of Cybersecurity*, columnforsec..com, March 8, 2016
- *The Human Element of Computer Security*, Robert Moskowitz, rsaconference.com, May 25, 2015
- *How to Secure Data by Addressing the Human Element*, Thor Olavsrud, ("When it comes to security, humans are low-hanging fruit"), cio.com, August 15, 2012
- *The Human Element in Cybersecurity Attacks*, Francie Diep, psmag.com, April 15, 2015