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 ominous threat is caused by the exponentially increasing amount of data across 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 Wi-Fi.

HUMAN ELEMENT OF DATA PROTECTION

People cause breaches. Examples of non-malicious cases 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.
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

- 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.

Emerging consensus on how 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, limits what types of emails can be sent, setting triggers and alerts when sensitive data is transmitted via email.
Establish written policies for data protection.

HUMAN ELEMENT OF DATA PROTECTION

Training is key.
- Training should be easy to understand and relevant to the particular audience.
- Ongoing, situational training—utilize an incident as a training tool.
- Make training fun and relevant. Consider using volunteers as real-life scenarios, break-out sessions, etc.
- 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, "tip something if you see something."
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 said 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 children’s names.
- Increasing use of biometric authentication, via fingerprints or derived credentials from card or phones.

HUMAN ELEMENT OF DATA PROTECTION

Finally, you should ensure that your organization has a comprehensive, cross-functional, incident response team to:
- (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:
- Case study: How to prevent data breaches, Info Security: Global, June 13, 2017
- The risks of insider threats, Info Security: Global, December 11, 2017
- The Human Element of Cybersecurity, RSA Conference, May 24, 2015
- The Internet Economy (2017), Deloitte, January 1, 2017
- The Human Element of Cybersecurity (2017), IBM, August 11, 2015
- The Human Element of Cybersecurity (2017), PwC, September 14, 2017
- The Human Element of Cybersecurity (2017), Accenture, October 17, 2017
- The Human Element of Cybersecurity (2017), Tata Consultancy Services, October 20, 2017
- The Human Element of Cybersecurity (2017), KPMG, November 10, 2017
- The Human Element of Cybersecurity (2017), Deloitte, December 22, 2017
- The Human Element of Cybersecurity (2017), Accenture, December 29, 2017
- The Human Element of Cybersecurity (2017), PwC, December 31, 2017
- The Human Element of Cybersecurity (2017), Deloitte, January 1, 2018
- The Human Element of Cybersecurity (2017), Tata Consultancy Services, January 10, 2018
- The Human Element of Cybersecurity (2017), KPMG, January 18, 2018
- The Human Element of Cybersecurity (2017), Deloitte, February 2, 2018
- The Human Element of Cybersecurity (2017), Accenture, February 14, 2018
- The Human Element of Cybersecurity (2017), PwC, February 28, 2018
- The Human Element of Cybersecurity (2017), Deloitte, March 9, 2018
- The Human Element of Cybersecurity (2017), Tata Consultancy Services, March 28, 2018
- The Human Element of Cybersecurity (2017), KPMG, April 10, 2018
- The Human Element of Cybersecurity (2017), Deloitte, April 18, 2018