Team: Team 3

Inject Number: 29

Inject Duration: 90 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 09:51:38 -0500

From: Chief Information Security Officer (CISO)

To: IT Staff

Subject: [P-100] Create Sensitive Data Policy

The CIO is concerned about our proprietary, sensitive, and personally identifiable information (PII) and the implications of cyber attack. His friend, the CEO of another company, had a data breach and has been under fire by the board after the cyber actors stole intellectual property and the PII of all their customers. To make matters worse, the company in question also has had multiple class actions filed today by the law firms representing the customers, which resulted in firing of the CEO and the CIO.

Taskers

1) The CIO has tasked us to create a detailed policy in a formal document for the appropriate use, protection (storage and transmission), and disposal/destruction of our sensitive, proprietary, PII, etc. information in all forms (paper, media, backups, cloud, phone). The policy must:

a) Define the authority for the policy (legal, corporate) the CEO has said he will sign it with the CIO being the responsible official for policing and enforcement. It shall take effect immediately upon issuance.
b) Define who is subject to the policy (don't forget to include partners and contractors)
c) Define sensitive information and list examples
d) Define media covered
e) Define protection requirements/mechanisms (such as: appropriate labelling, redaction, encryption, secure wipe, lock & key, contractual agreements, interconnection agreements, etc.)
f) Training Requirements
g) Define the consequences for failure to comply.

2) The final component of the task is to provide the CIO, via a separate memorandum, a few recommendations on what technical mechanisms we

could implement in the future to identify, categorize, and protect our information as well as detect information leakage or compromise (this includes existing and future capabilities).

Example for types of sensitive information and labels:

Company Policy xxx requires all documents to contain header and footer labels that define the classification level of the information within the document. Our company will use these three levels to define our data classification: public, business use only, and confidential.

The public classification label applies to information that is available to the general public and intended for distribution outside an organization.

Business use only classification label applies to information that is used within business processes, and the unauthorized disclosure, modification or destruction of which is not expected to seriously affect the organization, customers, employees or business partners.

The confidential classification label applies to information that is used in sensitive business processes, the unauthorized disclosure, modification or destruction of which will adversely affect an organization, its customers, employees or business partners.

Further Guidance: NIST special publication NIST 800-60 volumes 1 and 2, The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) publication ISO/IEC 27002:2013 8.2.1 provides further guidance for handling sensitive information.

Thank you.

Chief Information Security Officer (CISO)