CYBER SECURITY TRAINING

Training | Reinforcement | Testing

Scott Vanatter | Director, Business Development | 703-953-2535 x102 office | 703-395-6020 cell | scott@delviom.com

The Challenge

The average cost of a data breach in 2019 is 3.92 Million (ref- IBM). Studies have shown that over 90% of breaches have occurred due to human errors. Humans are the weakest link in terms of an organization's cybersecurity posture. Despite extensive processes, cyber-defense mechanisms, and IT investments, humans are still the easiest entry points for phishers.

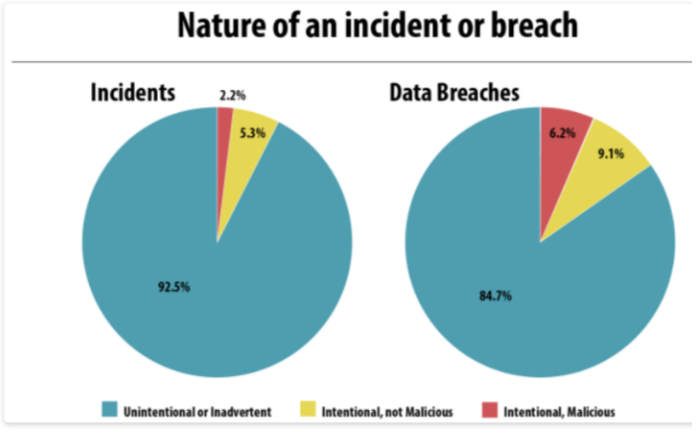
We can no longer ignore the importance of training employees on cybersecurity. Cyber Training empowers employees to protect themselves and protect their organizations by giving them the knowledge to recognize a threat.

Cyber training is a simple concept, yet it is difficult to implement successfully in practice. Why is that so?

- Dry subject matter
- Long winded approach
- Lack of consistency
- Lack of reinforcement
- Lack of testing

Verizon's 2019 Data Breach Investigations Report showed that 32% of the data breaches in 2018 involved phishing activity.

Furthermore, "phishing was present in 78% of Cyber-Espionage incidents and the installation and use of backdoors."



Source: Txmx 2

Delviom's Training Model

Delviom's Training Model is a holistic methodology to provide practical content which is measured and reinforced consistently.

delviom
INSIGHT | ANALYTICS | SECURITY

The Delviom Difference

Training, Reinforcement, & Testing

We believe that Security Awareness is a continuous process, it needs to be reinforced and tested frequently. Delviom delivers awareness training in a web-based format in short, frequent bursts that are easy to absorb and implement in daily use. We use gamifying techniques to reinforce training. We keep the content fresh and current by introducing new training on a periodic basis. We can manage training selection, delivery and user compliance.

Delviom also performs phishing simulation by sending seemingly malicious emails in a safe manner to test user understanding. The results of these tests can lead to training adjustments to reiterate concepts.

Case Study

USDA Rural Development

At USDA NRCS and USDA RD, Delviom provided training support on various fronts.

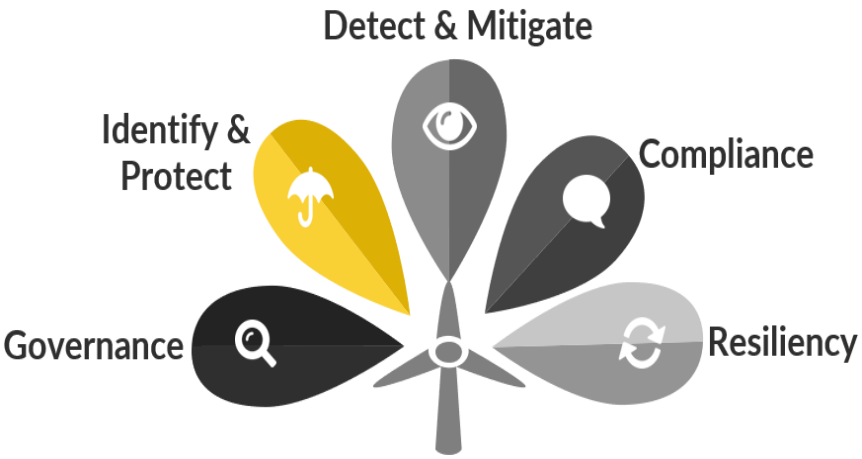
Delviom supported Security Awareness training including tracking metrics and maintaining compliance.

Delviom implemented several cutting edge technologies including Web Application Firewall (WAF), Threat Intelligence and Privacy mapping tools. We provided training on the above tools, processes and Standard Operating Procedures as we operationalized the tools and transitioned operations to the government.

We accomplished this via in-person training, shadowing activities and documentation. Training activities were a key to successful handoff at the close of the contracts.

Our Framework

Our robust Cyber Security Framework incorporates Security best practices with proven Governance principles to ensure “End to End” Cyber Security for your needs.



Our Clients

USDA
aps
GPO
GM
CollegeBoard
connect to college success
NEW MEXICO GOV
THE LAND OF ENCHANTMENT
IRS
ZIONS BANK
BlueCross BlueShield
FINRA
Kubota
REGENERON
CISCO
bright house NETWORKS
SANOFI
U.S. Citizenship and Immigration Services
Malt O Meal
Fidelity INVESTMENTS
FANATICS

SBA 8(a) Certified · ISO 20000 · ISO 27001 · ISO 9001:2015 · GSA IT Schedule 70 · CMMI SVC/3 · 8(a) STARS II · Great Place To Work. Certified · Certified WBENC Women's Business Enterprise