The Importance of INFORMATION SECURITY *for* BANKS

SOCIAL ENGINEERING ATTACKS AGAINST BANKS

90% In an industry study, 90% of those successfully exploited during an unauthorized facility entry trusted the intruder because they thought she worked for their company. (CSO)

28% Over 28% of phishing attacks detected in 2014 were against banks, payments systems and e-commerce companies. (Kaspersky Lab)

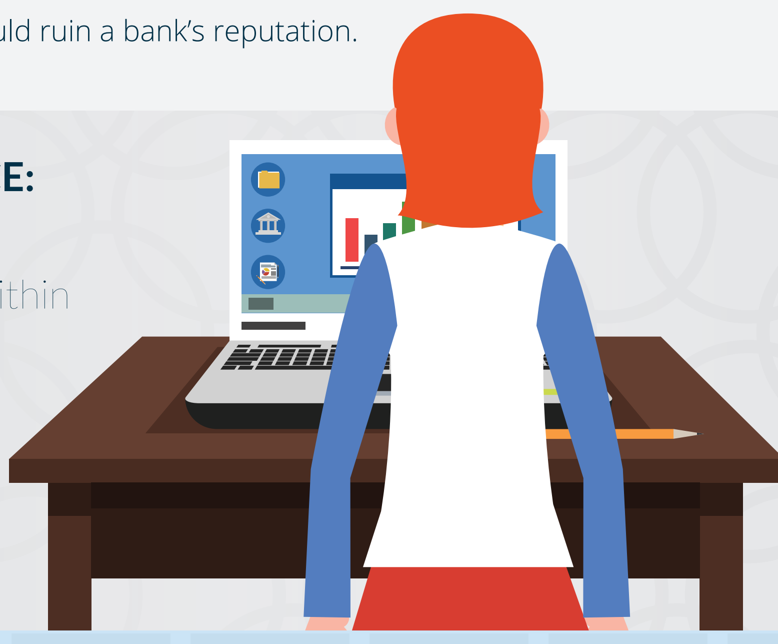
Why banks need information security options

The FDIC and OCC have tightened information security controls for banks, and FFIEC examiners are closely monitoring how banks are protecting customer information and accounts. In addition to these increased compliance standards, banks are feeling added pressure from customers and competition. Information security threat awareness is at an all-time high, and the demand for protecting sensitive data is increasing every day. All eyes are on the banking industry, and one false step could ruin a bank's reputation.

TIME IS OF THE ESSENCE:

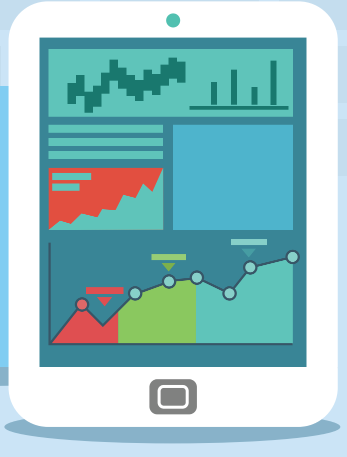
50% of opened and clicked **phishing emails** happen within the **first hour**, leaving little time for an effective response. (DBIR 2015)

A system is only as safe as the people controlling it.



$52,000 - $87,000 is the forecasted range of an average loss for a breach of 1,000 records. (DBIR 2015)

$259 is the average cost of each record exposed in the financial industry. (IBM)



Improving Your Information Security Program

IT Audit

An IT Audit should meet more than just your compliance requirements. It needs to review how your security controls are designed and implemented, while providing insights to potential gaps in your process or procedures. This practice improves the effectiveness and efficiency of your business security.

Vulnerability Scanning

A vulnerability scan is a tool used for finding the weaknesses in your computers, devices, networks and applications. Scans are often performed monthly to search for cracks in your security armor.

Penetration Testing

A penetration test is an ethical version of hacking your business. It is used to identify exploitable vulnerabilities, find potential data leakage and assess the effectiveness of your company's security program.

Social Engineering

Social engineering relies profoundly on human interaction and often involves misleading employees into violating their own company's security rules. Here are some social engineering tactics that threaten organizations.

Pretexting Phone Calls
Using a phone call to solicit information or setup an employee to be more receptive to a future attack

Phishing Emails
Sending an authentic looking email in attempt to steal personal and/or financial information

Unauthorized Facility Entry
Entering a facility without permission to discover what a non-employee has ability to access

Dumpster Diving
Searching in a facility's dumpster for private information that could be used in a malicious attack

Security Information & Event Management

Security Information and Event Management, or SIEM, involves collecting network and device logs in a centralized environment in order to correlate, consolidate, identify, analyze, alert and report security incidents.

Breach Investigation & Incident Response

In a breach investigation, it's imperative that expert guidance with experience in data recovery and preservation of evidence is provided to prevent spoliation of evidence.

Information Security Consulting

At Integrity we understand the unique demands of the banking industry. The members of our knowledgeable team have been providing information security services to banks for the past decade. We have served organizations ranging in size from the largest national banks to the smallest community banks across the country. Our services help banks fulfill IT compliance regulations as well as strict information security goals.

www.integritysrc.com | 515-965-3756

Integrity
SECURITY | RISK | COMPLIANCE

Sources
Kaspersky Lab - https://securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf
CSO - http://www.csoonline.com/article/2864598/security-awareness/the-2015-social-engineering-survival-guide.html
2015 Cost of Datat Breach Study
Verizon 2015 Data Breach Investigation Report (DBIR)