**The National Bank of Blacksburg Data Breach**

* National Bank of Blacksburg: a public bank in Virginia that offers banking, loan, mortgages, and credit card services.
* Hacking/malware Breach category
* Composed of 2 breaches both caused by a phishing email attack.
  + The first attack occurred on May 28, 2016 when hackers got access to the Bank’s STAR network by installing malware on an employee’s computer
  + The second occurred on Jan 7, 2017. This time hackers also regained access to the STAR network via the same method
* Hackers stole a total of $2.4 M in both incidents by dispensing fraudulent credits utilizing hundreds of ATMs.

**Vulnerability & Failure in controls**

* The organization and employees must be vigilant in knowing what a phishing attack looks like and prevent it.
* Employees must be aware of social engineering attacks – There should be regular and effective employee trainings.
* Failure in control: Hackers altered and removed critical security controls (PINS, daily withdrawal limits) by compromising the network.

**Control Recommendations**

* Before applying any controls, identify those Employees with information security roles and responsibilities and making sure that they have the right skill levels needed to perform information security duties through various training programs
* Additionally, the vulnerabilities scanning should be implemented to rank vulnerabilities according to their impact. Thus, these vulnerabilities shouldn’t be neglected, and the serious vulnerabilities that can be exploited by hackers are remediated.
* Furthermore, Pen testing: an in-depth analysis of weakness in the network & systems helps to rank vulnerabilities. Rigorous and proper pen testing could have identified the bank’s resistance ability to further phishing attacks to gain access to the network and prevented it from happening again.
* When it comes to protection, a better authentication of customers: for example, should require the customers to provide additional authentication information and hence decrease the probability of an attacker imitating them.
* Another one is Network segmentation: The organization needs to physically separate the corporate network into multiple subnetworks with managed interfaces. Internal networks and resources should be protected from threats that reside on the external network. This can be accomplished with firewalls, gateways, or routers and controlling the flow of connections to corporate computers.
* Employee training: Make sure employees are continuously trained on social engineering attacks such as phishing, and strongly enforce information security-related policies and procedures.
* Continuous monitoring with appropriate techniques allows identification of threats.
  + This includes checking if controls are working correctly
  + Once identified, malicious code execution can be prevented by as antivirus or other software products at information system entry and exit points (e.g. electronic mail servers, web servers, remote-access servers) and workstations
* Lastly, respond to the breach according to the Bank’s incident policies
  + The bank should analyze the forensics results
  + Lessons learned: Importance of access control testing, employee security awareness for quick detection of future intrusions and helps develop appropriate mitigation measures.

**Boeing Data Breach [Unintended Disclosure (DISC)]:**

* Occurred when an employee of the company sent a spreadsheet that contained personally identifiable information (PII) of 36,000 workers in an email on Nov 21, 2016.
* He sent it to his spouse (who doesn’t work there) to help him with formatting of the data
* Information contained are SSN, DOB, Employee ID, Full Name, Place of Birth, Accounting Department Codes
* Cost of breach might be as high as $5.7 M

**Vulnerability**

* Lack of DLP software
* Lack of adequate employee training

**Control Recommendations**

* Azure information protection (AIP) helps with classification of data for protection regardless of where it is stored or with whom it is shared. E.g. Financial Info data
* Labels (secret, top secret etc.) can be applied manually by employees, automatically by administrators who define rules and conditions, or a combination of both.
  + For example, you can configure a document that contains sensitive information to be accessed only by individuals within the HR department and control whether the document can be edited, restricted to read only or from being printed.
  + emails can be configured to prevent employees from attaching such documents or forwarding emails that contain the sensitive attachments.
* DLP: There are essentially the technologies that provide remediation for data loss based on content inspection and contextual analysis of data that is at rest, in motion, and in use.
  + They identify violation of policies (once set up in office 365 security & compliance center) defined by an organization or the ones the organization must company with such as HIPAA and PCI-DSS. It also provides reporting to meet compliance and auditing requirements
  + Policy automatically applied to contents that match the conditions in the policy
* Employee training: An information security program that highlights the sensitivity of data, the importance of information security, and stresses information security policies and procedures is an effective way for employees to understand policies and procedures.
* Microsoft Cloud App Security allows organizations to create anomality detection policies and utilize behavioral analysis to obtain real time detections targeted at prohibited employee activities.
  + Based on the policy results, security alerts are triggered when some action occurs that is different from the set employee privileges by the organization
* Incident analysis to
  + best understand the scope and impact of the breach that occurred so that an appropriate response plan can be established.
  + prevent further expansion of the incident, contain, and eradicate the exposed sensitive spreadsheet.
* Lessons Learned: rigorous controls and employee training should be given attention to in order to prevent employees inadvertently leaking sensitive personal information.

**Tesla Data Breach [Insider Attack (INSD)]:**

* Occurred beginning of due to a disgruntled employee using his credentials to export the company’s information such us
  + Trade secrets, financial information, manufacturing systems operation
* The employee essentially altered the company’s OS system by making code changes
  + Code was deployed on various systems and was designed to frequently send data even after he leaves Tesla
  + He was able to download large gigabytes of data and export it to 3rd parties
  + Tesla filed a lawsuit against him for $167 M in damages

**Vulnerability**

* + Lack of insider monitoring

**Control Recommendations**

* Identify, track, and monitor key assets and system resources to resist exposure to insider attacks. Who has access to what type of data & systems, what do they do with it?
  + Allows to be able to respond faster with more precision to mitigate incidents.
  + Monitoring shouldn’t be limited to privileged employees only since an inside attack can be launched by any user who Is associated with sensitive information.
  + Besides real-time monitoring, a report should also be provided by security professionals based on the accumulated logs that can be traced back to a specific employee
* Access control framework should be composed of
  + safeguards, separation of duties and recommended actions for security professional to utilize in order to minimize security risks and exposure.
* Specific deterrence controls include Data Loss Prevention (DLP), Identity and Access management (IAM), and encryption of data whether it is at rest, in motion or in use.
  + Helps identify any deviations from typical employee behavior such as reading large amounts of data than usual.
  + Helps address abnormal or risky employee behavior before a major damage occurs.
* Insider Monitoring and enforcing policies: Detecting unusual employee behaviors such as
  + below average work, hostility towards other employees,
  + coming in late and leaving early
  + working outside normal business hours, declining performance, and passive-aggressive behavior
  + Policies: Least privilege (limit access right to the bare minimum they need to perform their job) & hiring process (background checks)
* Fostering a culture of open discussion: The disgruntled employee in Tesla felt unvalued and thought his handwork was going by unnoticed.
  + initiating a conversation with such employees, asking for their opinions, encouraging them to open-up, and sincerely listening to their concerns and taking their viewpoint into consideration are essential to know their behavior and goals.
* Detection controls
  + Tools like IDSs monitor network traffic and alert any suspicious activity.
  + IPSs function in the same way by inspecting network packets and alert administrators about attack attempts.
  + They can both block suspicious packets and respond to potentially malicious network traffic and generate logs.
  + SIEMS aggregate the logs provide the ability to analyze log and event data in real time and report log data and malicious activity alerts to help security professionals monitor threats and respond to incidents. Security team should not be negligent of logs!
* Incident analysis to
  + best understand the scope and impact of the breach that occurred so that an appropriate response plan to continue business can be established.
    - Utlize forensics investigation result to determine what operations adjustments to make
* Lessons Learned: Even though it may seem hard to imagine that a trusted employee can do damage to his or her own organization, Tesla should note that it lacks tight controls, effective monitoring, and open discussion with employees.