Norfolk Southern Cybersecurity Assessment

Lawrencia Agyemang

Tre Bagby

Rafael Figueroa-Medina

Steven Miller

DISCUSSION POINTS

Today's presentation will cover the following information pertaining to Norfolk-Southern:

- Company Profile / Industry Info
- Asset Rankings
- Risk Management Matrix
- Key Performance Indicators
- Asset Recommendations

ABOUT THE COMPANY

Based out of Norfolk, Virginia, Norfolk Southern Corporation is the parent entity of the Norfolk Southern Railway Company major freight railroad. Collectively known as Norfolk Southern, they operate just over 35,000 miles of track across 22 states. With their operational footprint ranging from the Eastern seaboard to areas of the Midwest, they transport a wide variety of goods consisting primarily of raw materials, automobiles and automobile parts.

Norfolk Southern today was born from a rich history of the American railroad. In the late 1800's, the principal rail companies from the East consisted of the Southern Railway (formerly known as South Carolina Railroad Company) and the Norfolk and Western Railway. These early companies were at the forefront of railroad innovation, and are known for being the first to utilize the steam locomotive for passenger trains.

In 1982, these two companies were merged to form the Norfolk Southern Corporation. As the company continued to flourish, they were able to acquire other smaller (or larger, but floundering) rail companies, to include acquisition of over half of all assets from the Consolidated Rail Corporation (known commonly as Conrail), which alone added over 7,000 miles of track to their area of influence.

ABOUT THE INDUSTRY

Industry wide, The U.S. Freight Rail network spans over 140,000 miles of railway, and is operated by over 600 railroad companies. Made up of many “Class One” rail companies (revenues exceeding $500 million USD) and numerous short line or regional railroads, this network provides a cost-effective method of transporting various goods in a safe, timely manner. In 2020, railways accounted for transportation in excess of over 1.5 million tons of freight, and has been consistently increasing over the past 20 years.

In 2017 alone, freight railroads contributed $219 billion USD in economic output, as well as providing $71 billion USD in wages for over 1.1 million employees working within the industry. Supporting the nation’s critical infrastructure while employing over a million people, this industry is not only stable, but growing; the future looks promising.

ASSET RANKINGS:

Norfolk Southern, the major transporter of industrial products, is able to operate within the most extensive intermodal network in the Eastern coast because of their keen attention within various areas of their company. The following is a list of their Key Assets with a brief description of what they are and why they are important.

Value	Asset	Description	Explanation/Reasoning
1	Trade Secrets	Sensitive proprietary information like the formula used to reduce carbon and fuel usage within the locomotives	Trade Secrets widen the gap between the competition, and they can keep the company operating extremely efficient with an advantage over their competitors.
2	Train Tracks	Rail Network that is used to transit cargo and also leased to other companies for their use as well	Norfolk Southern's ownership of their rail network is why they control the majority of the railroads on the eastern coast of the United States.
3	IT Systems	Computer Systems and other IOT devices that are connected throughout their various networks	Protecting IT Networks is crucial for maintaining efficiency. Mitigating the risks involved with technology will not only reduce the success of a cyber attack, but it can also save the company millions of dollars and prevent a catastrophe that would be detrimental to the company.

4	Network Operations Center	The "Brains" of the operation. It is a control center which utilizes systems to command and control all aspects of the railway operations	Being the central point of all control measures, protecting this facility from both physical and cyber threats is very important to the company.
5	Personal Information	Information, both physical and digital that have worth.	There are several federal regulations in place that require safe and secure use when it comes to different kinds of personal information. Personal Information in the wrong hands can lead to a myriad of issues that will not only affect the company but also personnel throughout the company pending on the type of data.
6	Positive Train Control System	A system of functional requirements for monitoring and controlling trains in order to prevent mishaps from occurring	The PTC system is a regulatory requirement that needs constant monitoring. It contains critical data and is a bridge to several other networks and communications devices throughout the entire rail network.

7	Thoroughbred Yard Enterprise System	A system that generates a switching list to coordinate movement of cars from inbound trains to their outbound trains. Provides a graphic representation of how many cars are on each track, and how much room is left on the track to add more cars. Calculates optimum speed for cars to couple depending on weight of the cargo and controls of the braking systems on the track. Ultimately results in less damage to cargo and less yard accidents altogether.	Proper coordination of the several moving parts that are involved with each shipment is critical. Without a systematic approach, some cars can be lost or forgotten about, with valuable goods just sitting idle for a substantial amount of time. Things can even escalate and some of the different cars can be attached to the wrong train, and the goods will fail to reach their destination.
8	Employees	Personnel that are needed for both operations and maintenance. 18,500 personnel as of the end of FY 2021.	Employees are the heartbeat of any company. They make everything happen. Things like the recent pandemic can drastically reduce manpower which can affect the overall efficiency and security within the company, which ultimately affects the overall bottom dollar. Without the proper amount of personnel, the company cannot operate to its fullest capabilities, because there would be a shortage of personnel to produce the products which are logistics.

RISK MANAGEMENT MATRIX:

The following slides are the Summary cybersecurity risk assessment findings of Norfolk Southern Railroad. You will find both quantitative and qualitative methods of different assets.

TRADE SECRETS

The Executive Team is responsible and accountable for this asset, and they should consult with and inform the Legal Department.

- **Risk Descriptions** - Poor Training, Poor Physical Security Controls, Lack of Supervision/Management, Loss of Economic Value (Information becomes obsolete due to economic/technological advances.
- **Business Consequences** - The company can lose critical information that keeps them ahead of their competitors. Trade Secrets widen the gap between companies and how they run their respective businesses.
- **Severity Level** - 100
- **Likelihood** - 25%
- **Score** - 25
- **Mitigation** - Access Control, Monitoring Systems, Secure Devices/Equipment with more secure measures (i.e. BioMetrics, Two-Factor Authentication)
- **Contingency** - Regulatory Compliances

RAIL PROPERTIES

The Operations Team is responsible and accountable for this asset, and they should consult with the Finance Department and inform the Executive Team.

- **Risk Descriptions** - Physical Security, Poor Hazmat Program, Misuse of Equipment, Lack of Maintenance that leads to equipment failure.
- **Business Consequences** - Down train lines are not operational, and can affect delivery timelines, routes, and the overall reliability and mission of the company.
- **Severity Level** - 85
- **Likelihood** - 15%
- **Score** - 12.75
- **Mitigation** - Effective Hazmat/Maintenance Program, Training, Alternate Routes.
- **Contingency** - Alternate Routes, Adding a little lead time to account for potential delays during shipping.

IT SYSTEMS

The Information Technology Team is responsible and accountable for this asset, and they should consult with the Operations Department and inform the Executive Team.

- **Risk Descriptions** - User Error, Lack of Security in Systems, Unencrypted Data, Unsecure Third Party Services
- **Business Consequences** - Could seriously disrupt financial systems, to include critical financial infrastructure that can lead to instability implications. It can have a large effect on the country's economy as goods and services will not be able to be transported across the country.
- **Severity Level** - 95
- **Likelihood** - 11%
- **Score** - 10.45
- **Mitigation** - Update Software, Monitor for Data Leaks, Breach Response Plans, Better Password Policy.
- **Contingency** - Disaster/Emergency Recovery plans

NETWORK OPERATIONS CENTER

The Information Technology Team is responsible and accountable for this asset, and they should consult with the Operations Department and inform the Executive Team.

- **Asset Value** - $25,000,000
- **Exposure Factor** - 20%
- **Single Loss Expectancy** - $5,000,000
- **Annual Rate of Occurrence** - 0.33
- **Annualized Loss Expectancy** - $1,650,000
- **Total Cost of Ownership of Mitigation** - $147,500
- **Annualized Loss Expectancy w/o Mitigation** - $1,650,000
- **Return of Investment** - $1,502,500

THOROUGHBRED YARD ENTERPRISE SYSTEM

The Information Technology Team is responsible and accountable for this asset, and they should consult with the Operations Department and inform the Executive Team.

- **Asset Value** - $9,380,000,000
- **Exposure Factor** - 40%
- **Single Loss Expectancy** - $3,752,000,000
- **Annual Rate of Occurrence** - 1
- **Annualized Loss Expectancy** - $3,752,000,000
- **Total Cost of Ownership of Mitigation** - $526,667
- **Annualized Loss Expectancy w/o Mitigation** - $3,752,000
- **Return of Investment** - $3,225,333

TRAIN TRACKS w/ MAINTENANCE PLAN

The Information Technology Team is responsible and accountable for this asset, and they should consult with the Operations Department and inform the Executive Team.

- **Asset Value** - $42,200,000,000
- **Exposure Factor** - 2%
- **Single Loss Expectancy** - $867,040,000
- **Annual Rate of Occurrence** - 200
- **Annualized Loss Expectancy** - $173,408,000,000
- **Total Cost of Ownership of Mitigation** - $25,500,000,000
- **Annualized Loss Expectancy w/o Mitigation** - $422,000,000,000
- **Return of Investment** - $223,092,000,000

TRAIN TRACKS (Per Mile)

The Operations Team is responsible and accountable for this asset, and they should consult with the Finance Team while also being informed by the Executive Team.

- **Asset Value** - $2,000,000
- **Exposure Factor** - 100%
- **Single Loss Expectancy** - $2,000,000
- **Annual Rate of Occurrence** - 6
- **Annualized Loss Expectancy** - $12,000,000
- **Total Cost of Ownership of Mitigation** - $1,093,333
- **Annualized Loss Expectancy w/o Mitigation** - $12,000,000
- **Return of Investment** - $11,073,334

EMPLOYEES

The Operations Team is responsible and accountable for this asset, and they should consult with the Executive Team while also being informed by the Legal Team.

- **Asset Value** - $1,000,000
- **Exposure Factor** - 25%
- **Single Loss Expectancy** - $250,000
- **Annual Rate of Occurrence** - 5
- **Annualized Loss Expectancy** - $1,250,000
- **Total Cost of Ownership of Mitigation** - $516,000
- **Annualized Loss Expectancy w/o Mitigation** - $1,250,000
- **Return of Investment** - $734,000

KEY PERFORMANCE INDICATORS:

Listed below are a few of the major metrics that are tracked throughout the organization:

- Frequency of review of third-party accesses
- Frequency of access to critical enterprise systems by third parties
- Security Policy Compliance
- Revenue Ton Miles, Revenue per Revenue Ton Miles, Carloads
- Access Management

ASSESSMENT RECOMMENDATIONS:

- The following slides highlight the Company's "Top 8" and give a brief description and the recommended controls.

Trade Secrets and Intellectual Property Confidentiality & Non-Disclosure Agreements (Rafael Figueroa-Medina)

Norfolk Southern has developed many innovations in rail technology over the years, and as such owns patents for numerous proprietary equipment and software. Information involving Trade Secrets and Intellectual Property will be a large part of the employees' day to day duties; establishing boundaries of what can and cannot be done with this knowledge is crucial to safeguarding this vital information.

The category applied to this control is Protect, Data Security, and the appropriate sub-category being PR.DS-5: "Protections against data leaks are implemented". Establishing a control of Confidentiality and Non-Disclosure Agreements will mitigate any potential risks to the Company's Intellectual Property from spreading into the wrong hands. Non-Disclosure Agreements create the legal framework to protect ideas and information from being stolen or shared with competitors or third parties. Some of the language that would be implemented within these agreements, establishing what needs to be confidential, the scope of the confidentiality obligation by the receiving party, exclusions from confidential treatment, and the overall terms of the agreement.

Policy – Confidentiality and NDA compliance

All employees and trusted partners must adhere to and sign the organization's confidentiality and non-Disclosure agreements.

Procedure

Due to the nature of our business and the frequency personnel might be exposed to and/or work with sensitive intellectual property, it is crucial that safeguards are implemented in place to protect from potential attacks. All personnel employed within the company, to include our partners who frequent our premises will sign these agreements, acknowledging that they may or may not have access to sensitive information like trade secrets and/or intellectual property. Individual Personnel are responsible for signing and maintaining a personal copy of the applicable forms.

The IT Security Division will be responsible for maintaining a database record with all the signed agreements. They will also be responsible for drafting quarterly and annual reports to be submitted to the IT Department & Administrative Department Leads.

Review Frequency

The Confidentiality & Non-Disclosure Agreement Policy will be reviewed annually by the IT & Administrative Departments. The findings from the review meetings will be submitted for approval to Senior Management. This submission will be due no later than the last Friday of the current fiscal year.

Video Surveillance of Train Tracks (Tre Bagby)

Norfolk Southern has approximately 70,000 pieces of rail spanning roughly 20,000 miles of track, along with associated switches, crossings and communications equipment. Closed-circuit surveillance cameras, security guards, and motion sensors will have a major positive impact on safety and monitoring of this equipment. The possible controls for our Train Tracks that are expanded across the Eastern Shore, Eastern United States, and continuing onto the Midwest are numerous; These tracks that run through each state we operate in need to have in place mitigations, protections, and deterrent type of controls.

The category applied to this control is Detect, Security and Continuous Monitoring (DE.CM), and the appropriate sub-category being DE.CM-7: “Monitoring for unauthorized personnel, connections, devices, and software is performed”. These surveillance cameras will be needed to detect suspicious activity on our property, internal or external to either turn away criminals or capture a person in the act of doing malicious activity. The security guards will be able to provide a physical presence.

Policy – Surveillance Monitoring

All tracks will have a closed-circuit surveillance camera system that will be centrally controlled at the main distribution site for Norfolk Southern Corporation. Whether it be a checkpoint, anywhere on the track through any state, within the length of half of a mile there will be a security camera placed North and South, or East and West of the direction that the train is headed. If a checkpoint site is without a security camera surveillance system, there would be a different type of surveillance in place, whether it be physical security guards or even motion sensors that will act as security cameras to the point where we can have an alternate control to protect these assets.

Video Surveillance of Train Tracks (Tre Bagby) (Cont'd)

Procedure

The operations and security department will be responsible for putting the correct types of controls for camera surveillance, and or security deterrence. They will be responsible for the installing and maintaining of these controls to safeguard the company and this type of asset of such large monetary value. To verify these controls the security and operations departments will conduct security checking monthly to make sure that all devices and or guards are aware of the climate change that is to come, or if they have any security policies that have changed. The number of guards, cameras, and or sensors will be documented as to where they are per location, and what their duty is supposed to be. As they are documented, the results will go up the chain of command. If there were no faulty outcomes within the month, then procedure continues as nothing has changed. However, if there were issues with how the cameras were responding to criminal activity, or if the motion sensors did not pick up any behavior that was unusual, they would be under review which may result in the device being terminated.

Review Frequency

The Security policy will be reviewed on a monthly basis, with a report given to the higher chain of command. The completion of the review will result in devices or employees that have good standards, fault, and or will require termination will be reviewed upon the end of the monthly check in.

Internal and External Cybersecurity Risk Assessment of the IT Systems (Rafael Figueroa-Medina)

Norfolk Southern's IT systems are heavily integrated throughout the entire organization. Knowing and understanding vulnerabilities within our infrastructure is crucial in developing methods the organization will utilize to monitor and safeguard against these vulnerabilities. Risk Assessments are processes that evaluate hazards, and then remove that hazard or minimize the level of its risk by adding control measures as necessary.

The category applied to this control is Identification, Risk Assessment (ID.RA), and the appropriate sub-category being ID.RA-1: "Asset vulnerabilities are identified and documented". The overall intent of these controls is to ultimately have a safe network in which personnel can conduct the company's business without the fear of being attacked from an internal or external entity. Companies tend to develop blinders over time, and can be naïve to potential flaws in their own designs. Having internal risk assessments is not enough; by contracting external companies to conduct risk assessments, the organization has an opportunity to better understand their own designs, while having fresh personnel look for potential flaws in their system.

Assuming budgetary constraints are an ever-present obstacle, these assessments assist in prioritizing what areas require more attention than others. This results in a company able to better understand how to prioritize spending to protect their infrastructure, all while in a format where it can be easily understandable to non-technical personnel.

Internal and External Cybersecurity Risk Assessment of the IT Systems (Rafael Figueroa-Medina) (Cont'd)

Policy – Risk Assessment Policy

The purpose of this policy is to empower the IT Security Team to perform periodic information security risk assessments for the purpose of determining areas of vulnerabilities, and to initiate appropriate remediation. The policy will also ensure that the organization is taking the proper steps and procedures to meet regulatory guidelines like HIPAA, Sarbanes-Oxley, PCI DSS, and others.

Procedure

The IT department will conduct internal risk assessments quarterly; A comprehensive risk assessment of the IT infrastructure, applications, and technology will be conducted by a third-party organization at a minimum of once per year. Risk assessments can be conducted on any information system, to include applications, servers, networks, and any other process or procedure by which these systems are administered and/or maintained.

The execution, development, and implementation of remediation programs is the joint responsibility of the IT Security division and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any risk assessment being conducted for which they are held accountable. Employees are further expected to work with the risk assessment team in the development of a remediation plan.

Review Frequency

The Cybersecurity Risk Assessment Policy will be reviewed annually by the IT & Administrative Departments. The findings from the review meetings will be submitted for approval to Senior Management. This submission will be due no later than the last Friday of the current fiscal year.

Controlled Access to Ops Center Critical Systems (Steven Miller)

The Network Operations Center (NOC) was previously identified as an asset that falls under the Protect risk function. Being that the NOC is the central controlling station for all day-to-day operations of automated systems, maintaining security of access to the numerous systems within the facility is critical to ensure continued, safe operations.

The category applied to this control is Identity Management, Authentication and Access Control (PR.AC), and the appropriate sub-category being PR.AC-4: “Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.” Ensuring that only authorized personnel are accessing these systems (only when necessary) is key to mitigating any system interactions that might result with negative consequences.

Policy – “Need to know” and “as required” access and permissions.

Job titles and specific positions will be identified and assigned to personnel as required; Access gained to any system will only be in effect only as long as designated personnel are assigned to work within that system.

Controlled Access to Ops Center Critical Systems (Steven Miller) (Cont'd)

Procedure

Norfolk Southern employs numerous computer systems to facilitate autonomy throughout the rail network. From logistics planning to automated safety measures, any disruption or damage to these systems could be catastrophic to daily operations. In order to mitigate potential interruptions:

Management / HR will update employee records to reflect current work assignment to establish "need to know" authority to gain access to their respective computer system (ie, Movement Planner, Positive Train Control, Crew Management system, etc.)

The IT department will generate Role-Based Access accounts in accordance with "need to know" authorization found in employee files.

Upon employee reassignment/termination, Management / HR will IMMEDIATELY update employee files, and inform IT department of employee's change of status; IT department shall then revoke any access to computer systems the employee no longer has a "need to know".

Review Frequency

On a monthly basis, representatives from both HR and IT departments shall work together to verify all access permissions currently in effect match the requirements needed for each employee (depending on what system they are currently assigned to).

Access Permissions to Personal Information (Company and Financial) (Lawrencia Agyemang)

From employee Social Security numbers to Vendor Accounting data, Norfolk Southern has a very broad range of sensitive information to protect. Restricting access to sensitive personal and company information (and understanding why) will be an integral part of Norfolk Southern Railroad's defense mechanism against information getting into the hands of unwanted persons.

The category applied to this control is Protect, Awareness and Training, and the appropriate sub-category being PR.AT-2: "Privileged users understand their roles and responsibilities." The control will be across board and will cover all aspects of protection, especially where the data is stored in the company's systems and can easily be compromised when a virus, and other harmful programs get access to the company.

Policy

It will be a requirement at Norfolk Southern Railroad for all employees to be trained on information access. They will be trained on access and non-access information and why some information is restricted. They will also be required to adhere to all requirements regarding sharing information, speaking to the media or journalists as well as clicking links that may be deemed dangerous to the company. The employees will also be held liable for any company information leaked outside and was under their care.

Access Permissions to Personal Information (Company and Financial) (Lawrencia Agyemang) (Cont'd)

Procedure

The HR and IT department have the responsibility to train all employees on protecting the company's information. The two departments will help employees on what is deemed secret and what is not. Further, there will be HR manual booklets which will further aid in helping protect the company's information. The training will also entail how to use the company's information and to what extent. In matters IT and company information, sharing with third parties will also be limited. Further, the training will cover how to use anti-malware to protect against phishing attempts and other data-mining attempts for malicious reasons.

Review Frequency

Human Resources and Executive department representatives will meet annually to assess effectiveness of training programs and further discuss policy revisions.

Positive Train Control (PTC) checks (Lawrencia Agyemang)

Safety of trains in motion is paramount to both human lives and cargo delivery. Positive Train Control systems are designed to prevent a myriad of issues regarding the trains, to include train-to-train collisions, over-speed derailments, incursions into established work zones, and movement of trains through switches left in the wrong position.

The risk category applied to this control is Protect, Data Security (PR.DS), and the appropriate sub-category being PR.DS-8: “Integrity checking mechanisms are used to verify hardware integrity”. Although there are already federally mandated regulatory controls implemented within this system, establishing a local routine of training in actual live scenarios will ensure the efficiency of the PTC system program. It is vital to have all essential personnel applicable to this system to understand their roles within this process to include applicable third-party stakeholders in order to have a smooth process. If this program isn’t practiced frequently, it can lead to a lot of different confusion and will most likely lead to an increased chance of being able to prevent a mishap if the situation were to present itself.

Policy – Positive Train Control Requirements Policy

The purpose of this policy is to establish the requirements involved within the Positive Train Control System. Positive Train Control systems are designed to prevent train-to-train collisions, over-speed derailments, incursions into established work zones, and movement of trains through switches left in the wrong position. This policy will outline what is required, to include the frequency in which this system is simulated in order to maintain proficiency

Positive Train Control (PTC) checks (Lawrencia Agyemang) (Cont'd)

Procedure

This system is required to be monitored 24 hours a day, 7 days a week in order to prevent any accident that may occur. In addition, there will be daily checks that must be done each day to ensure the successful execution of the program.

Each applicable department will have a role to play in order to have a safe and successful execution of this policy.

The Network Operations Center will establish communications with the base stations that control the corresponding signal switches to the locomotive.

The Communications Department will ensure the proper functionality of signaling systems prior to the train departure by corresponding with the Network Operations Center and train engineer.

The Train engineer is responsible for monitoring the instruments that measure air pressure, speed, battery power, and other vital controls for the locomotive.

The wayside unit monitors and reports switch positions and signal indications to both the locomotive computer and Network Operations Center. The locomotive computer accepts the movement authority and speed restriction information and compares them against the train's location to ensure compliance. PTC also enforces braking or speed reductions when a train is approaching a segment of track occupied by another train, work zone, or misaligned switch.

Review Frequency

The Positive Train Control System Policy will be reviewed annually by the Network Operations Center and Signaling Department, or whenever there is a change in federal legislation regarding the system. The findings from the review meetings will be submitted for approval to Senior Management no later than 15 days after a change in legislation or the last Friday of the current fiscal year.

Thoroughbred Yard Enterprise System (TYES) and Responses following adverse events (Steven Miller)

The Thoroughbred Yard Enterprise System (TYES) is at the core of managing our train yards. This system generates a switching list to coordinate movement of rail cars from inbound trains to their outbound trains. It also provides graphic representation of how many cars on each track, and how much room is left on track to add more cars, as well as calculating optimum speed for cars to couple depending on weight of cargo and controls braking systems on the track. The ultimate goal of this system is to minimize damage to cargo by reducing yard accidents.
Although there are extensive control measures in place to ensure continuous, safe operations within the train yard, there still remains the possibility for negative actions to occur. When these instances happen, a correct and timely response is critical.

The risk category applied to this control is Response Communications (RS.CO), and the appropriate sub-category being RS.CO-2: “Incidents are reported consistent with established criteria.” Ensuring timely involvement of the authorities and providing them with all relevant data is imperative.

Policy – Notification requirements.

A timely response from law enforcement is critical to facilitating an effective investigation and prosecution of individuals responsible. This policy will outline the importance of compliance with law enforcement and shall provide guidance on what information shall be furnished to investigators.

Thoroughbred Yard Enterprise System (TYES) and Responses following adverse events (Steven Miller) (Cont'd)

Procedure

Following any adverse event involving TYES in one of our train yards

NOC shall be notified immediately after initial controlling responses (securing the area, safety concerns addressed, etc.).

NOC shall notify cognizant law enforcement agencies, as well as dispatch personnel from Norfolk Southern Police Department (if not already on scene). Public Affairs personnel shall also be notified/activated at this time.

NOC will dispatch operations personnel (with assistance from IT department personnel) to perform data analysis on all relevant computer systems and data logs present. Copies of all relevant data shall be generated and set aside, in order to be surrendered to law enforcement when requested.

Train yard personnel (with the assistance of Norfolk Southern Police) shall collect all video surveillance recorded during the adverse event and surrender to law enforcement when requested.

Review Frequency

Bi-annual policy review shall take place with personnel from both Management and Operations. A "Lessons Learned" memo shall be generated from adverse event reports from the current period; these memos will be used to affect changes to policy where needed.

Control: Employee Screening and Security Training (Tre Bagby)

Security Awareness Training will be able to help either regular employees or senior management have the ability to help find an internal or external threat before it will have an effect on Norfolk Southern Corporation. It will be important with the capability to train users the rights and wrongs of how to go about the day-to-day policy with information systems, physical security and so on.
The category applied to this control is Protect, Awareness and Training (PR.AT), and the appropriate sub-category being PR.AT-1: “All users are informed and trained”. Conducting this training for all employees (initial training for new hires, refresher training for current employees) is a proactive approach to potential adverse events; Employees gain critical understanding as to why we take certain types of precautions before it is too late.

Policy

All employees will be required to take a security awareness training that is a part of the yearly mandatory by the Norfolk Southern Corporation as well as the Department of Defense. Employees will be required to pass the Security Awareness Training; they will need to be responsible for watching all of the videos as well as answering any questions that follow the videos. Before employment a background check will be required for each and every employee regardless of seniority along with a briefing. Briefing will play a part with Human Resources and Security so that we are able to let the employee know what is acceptable within the corporation and what is not allowed when it comes to talking and information that is classified, or against policy. As to after employment, employees will need to be granted a debriefing. For Debriefing, employees that are soon to leave the company will need to be addressed to what is acceptable within the corporation and what is not allowed when it comes to talking and information that is classified, or against policy. If they are to not to follow any of these NDA’s, they will be prosecuted to the full extent of the law.

Control: Employee Screening and Security Training (Tre Bagby) (Cont'd)

Procedure

The Human Resources department will be responsible for sending out background check applications that will be conducted by any credible government agency that is credible and is completing them in a timely manner. Human Resources will conduct security awareness training annually to make sure that all employees are aware of the security procedures that are in place, or if they have had the chance to change. Human Resources will collect the certificates and keep the security training up to date and the months go on, as it will be tracked. As the certificates are collected on an annual basis, Human Resources will document the certificates that are on time, late, or not turned in. With regards to compliance, employees that do not complete this training will be penalized and HR will document this as they document the employees that have completed the training.

Review Frequency

The Security Awareness Training policy will be reviewed on a yearly basis, with a report given to the higher chain of command. The completion of on time submittals will be reviewed before the end of the fiscal year calendar.

CONCLUSION:

The list of assets discussed above are not all inclusive. As technology advances and the economy shifts, there can be new key assets that need monitoring and controls implemented in order to maintain productivity and success through an organization. Assessments like the ones done here, serve as a guide of understanding what vulnerabilities are out there, and how it can possibly affect a company. The results serve a purpose of hardening and improving an overall defensive posture that minimizes the potential damage from threats.