ETM 534 - TECHNOLOGY ROADMAPPING
SUMMER 2022

CYBER SECURITY ROADMAP FOR SYSTEM LOCKOUT AT PORTLAND GENERAL ELECTRIC (PGE)

Professor: Tugrul Daim

Presented by Team 3:
Elsamol, Amrutha, Haydar, Ned, Vaishali, Farzaneh

Portland State
UNIVERSITY

AGENDA

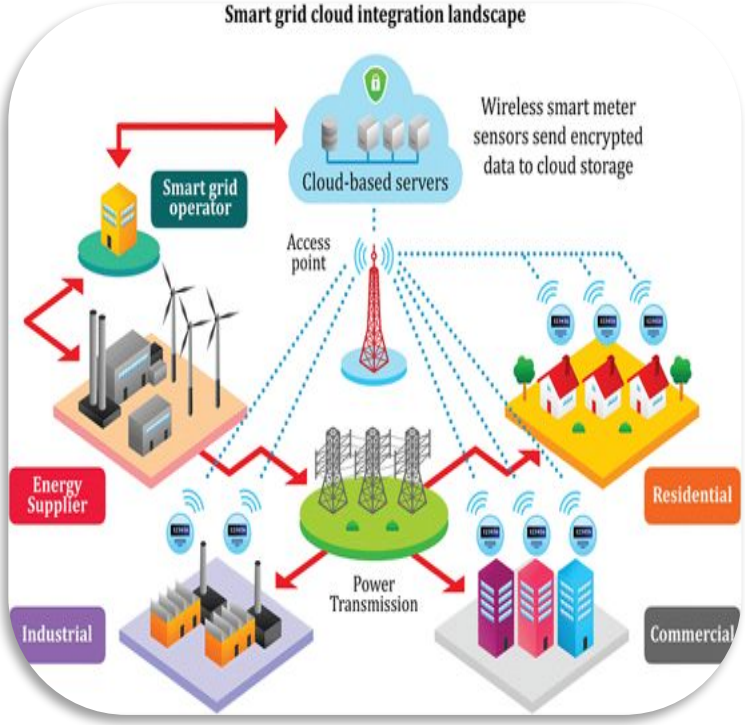
- Background
- Objectives
- Drivers
- Product Features
- QFD
- Gaps
- Technology
- Resources
- Roadmap
- Conclusion

BACKGROUND

Portland General Electric (PGE) is a Fortune 1000 public utility based in Portland, Oregon. It distributes electricity to 44% of the inhabitants of Oregon.

Founded in 1888 as the Willamette Falls Electric Company. It produces and purchases energy primarily from coal and natural gas plants, as well as hydroelectric power from dams on the Clackamas, Willamette and Deschutes rivers.

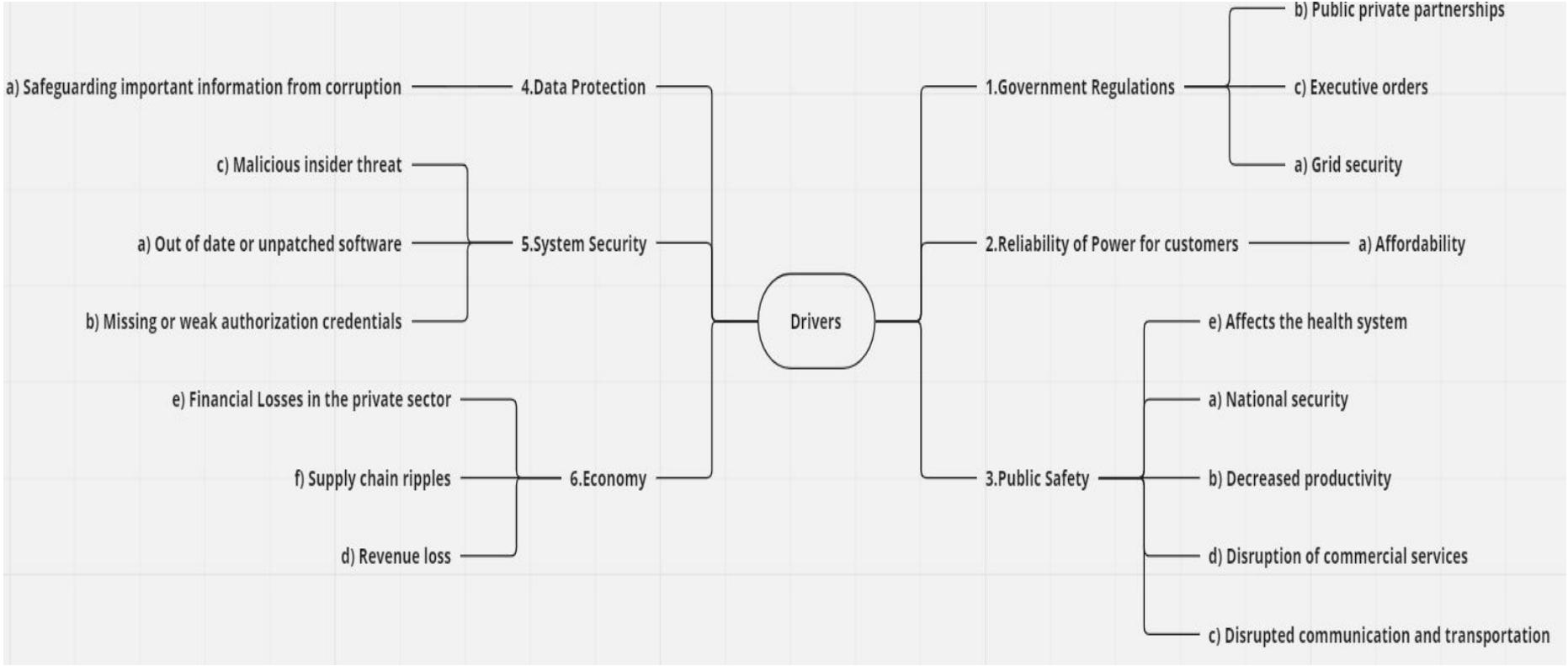
Since power grids span a wide geographic area, public and private networks can provide a communication path between remote sites and a control center. These capabilities also open doors for criminals, terrorists, “hacktivists,” and foreign governments to access a power grid and cause disruptions to the normal operation of the grid. This causes lengthy blackouts which can impact national security, public safety, and the national economy in a catastrophic manner.



OBJECTIVES

Work with Portland General Electric (PGE) to identify the complexity and challenges in cybersecurity that can be solved by incorporating system lockout methodology and develop a roadmap.

MARKET DRIVERS



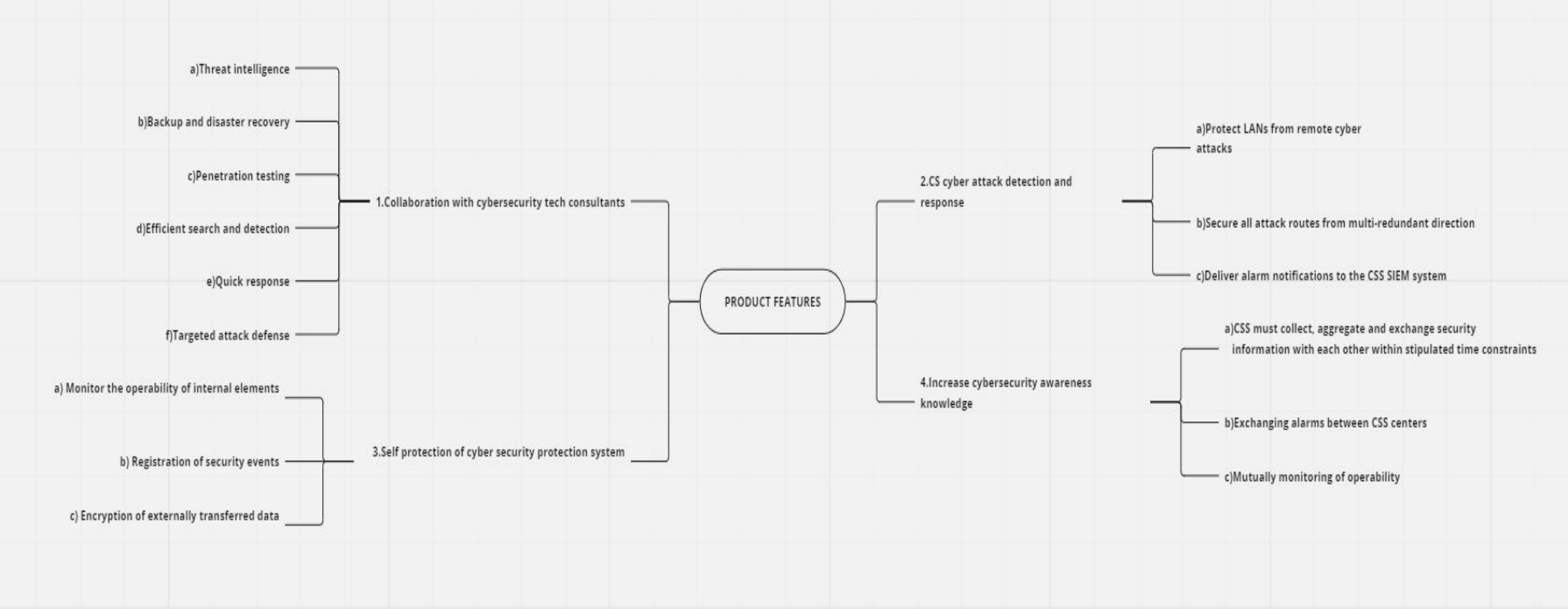
MARKET DRIVERS

Market Drivers	Category	Label	Driver	Definition	Weight
	Government Regulations	D1	Grid security	taking action to help this critical infrastructure (power grid) defend against the persistent cyber-attacks	4
		D2	Public private partnerships		4
		D3	Executive orders		4
	Reliability of Power for customers	D4	Affordability	PGE strives to provide a reliable electric supply	2
	Public Safety	D5	National security	Electricity is literally life saving technology When there is power outages, people are in danger	2
		D6	Decreased productivity		2
		D7	Disrupted communication and transportation		2
		D8	Disruption of commercial services		2
		D9	Affects the health system		2
	Data Protection	D10	Safeguarding information from corruption	process of safeguarding information from corruption or loss	4
	System Security	D11	Out of date or unpatched software	Electric utilities can be affected by cyberattacks across the whole value chain	4
		D12	Missing or weak authorization credentials		4
		D13	Malicious insider threat		4
	Economy	D14	Revenue loss	As electricity grids increasingly become smart the impact of a cyber attack becomes more severe and wide reaching	2
		D15	Supply chain ripples		2
		D16	Financial Losses in the private sector		2

DRIVERS TIMELINE

Drivers	Category	Driver	Now	2030	2040	2050
	Government Regulations	Grid security	grid security			
		Public private partnerships	public private partnerships			
		Executive orders		executive		
	Reliability of Power for customers	Affordability		affordability		
	Public Safety	National security	National security			
		Decreased productivity	decreased productivity			
		Disrupted communication and transportation	communication			
		Disruption of commercial services	commercial			
		Affects the health system	health system			
	Data Protection	Safeguarding information from corruption	data protection			
	System Security	Out of date or unpatched software	out of date software			
		Missing or weak authorization credentials	weak credentials			
		Malicious insider threat	insider threat			
	Economy	Revenue loss	revenue loss			
		Supply chain ripples	Supply chain ripples			
		Financial Losses in the private sector	financial losses			

PRODUCT FEATURES-MIND MAP



PRODUCT FEATURES

Product Group	Product Features	Definition
Collaboration with Cybersecurity tech consultants	P1: Threat intelligence	Data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.
	P2: Backup and disaster recovery	A mechanism that allows to recover the data loss and the recovery tools offering the consistent data backups to counter disasters.
	P3: Penetration testing	Conduct planned cyber-attacks on the system in anticipation of the possible threats to evaluate the security standards
	P4: Efficient Search and Detection	Cybersecurity protection system must raise alarms upon detecting anomalous IED
	P5: Quick response	Brisk investigation and response of security breaches to neutralize the immediately
	P6: Targeted attack defense	Shielding against targeted attacks on a system to prevent any damage
CS cyber attack detection and response	P7: Protect LANs from remote cyber attacks	Cybersecurity protection system must support the elimination of attacks by preventingdangerous network traffic from reaching the destination.
	P8: Secure all attack routes from multi-redundant direc	Network traffic that doesnot match the pre-configured patterns must be blocked
	P9: Deliver alarm notifications to the CSS SIEM system	Security modules must deliver alarm notifications to the CSS SIEM system.
Self protection of cyber security protection	P10: Monitor the operability of internal elements	Periodic "heartbeat" messages must be generated. Alarms must be raised when "heartbeat" messages from physical and software components are not received
	P11: Registration of security events	change in the everyday operationsof a network or IT service indicating that a securitypolicy may have been violated or a security safeguard may have failed
	P12: Encryption of externally transferred data	translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it
Increase cybersecurity awareness knowledge	P13: CSS must collect, aggregate and exchange security information with each other within stipulated time constraints"	Cybersecurity protection systemmust collect, aggregate and exchange security information on its state with other CSS cybersecurity protection systems on demand and within the stipulated time constraints.
	P14: Exchanging alarms between CSS centers	Translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it
	P15: Mutually monitoring of operability	Cybersecurity protection systems must mutually monitor the operability of other CSS systems
CSS engineering maintenance interface monitoring	P16: Substation resources must have secure access through a centrally supervised gateway"	Cybersecurity protection system mustimplement mandatory access control of users of engineering maintenance interfaces.
	P17: SCADA commands transmitted over an engineering maintenance interface must be monitored and alarms	SCADA commands transmitted over an engineering maintenance interface must be monitored and alarms generated in case of permission violations"
	P18: Mandatory access control for all devices accessed by engineering maintenance"	Cybersecurity protection system must provide mandatory access control for all devices accessed by an engineering maintenance interface based on a specified set of permitted IP addresses and time constraints

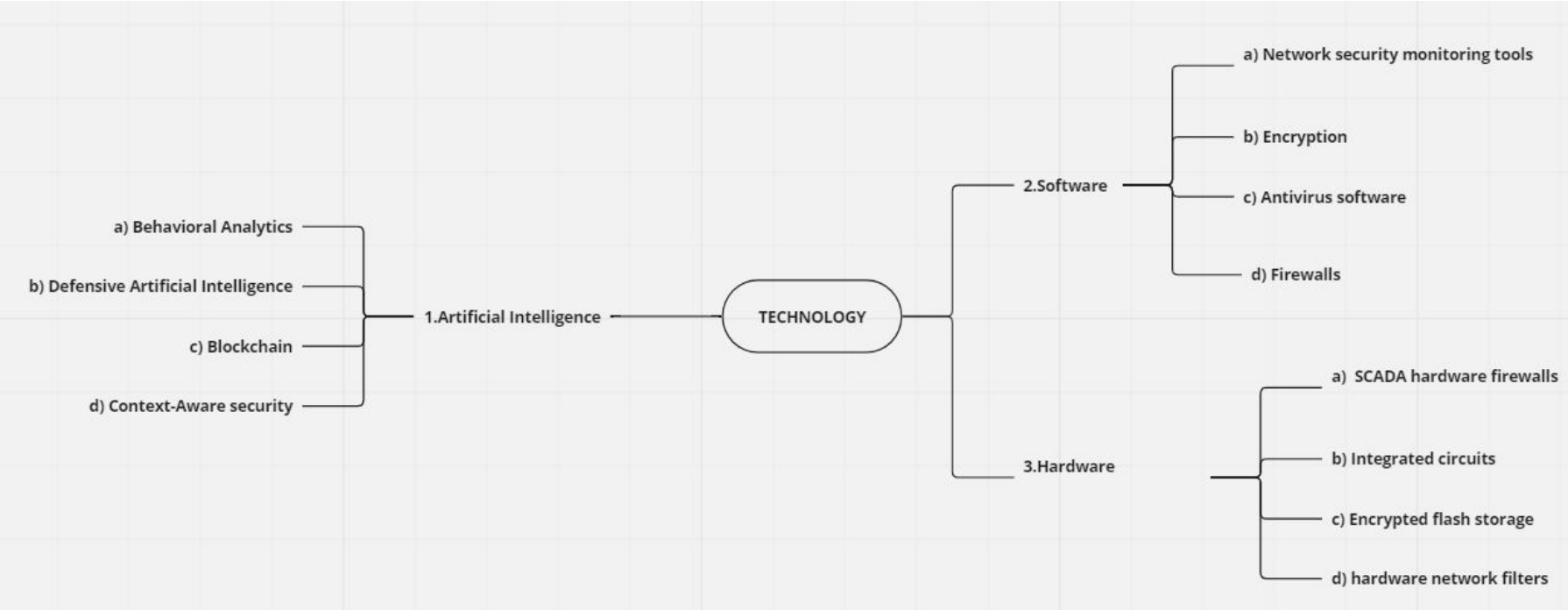
PRODUCTS AND DRIVERS QFD

Product Features \ Drivers	Weight	D1:Grid security	D2:Public private partnerships	D3:Executive orders	D4:Affordability	D5:National security	D6:Decreased productivity	D7:Disrupted commu and transportation	D8:Disruption of commercial services	D9:Affects the health system	D10:Data protection	D11:Out of date or unpatched software	D12:Missing or weak authorization credentials	D13:Malicious insider threats	D14: Revenue loss	D15:Supply chain ripples	D16:Financial losses in the private sector	Total
P1:Threat intelligence	2	4	4	4	2	4	0	1	0	0	4	2	2	4	0	0	0	62
P2:Backup and disaster recovery	4	4	0	0	0	0	2	4	2	0	4	4	1	1	2	2	1	108
P3:Penetration testing	2	4	0	0	0	2	1	1	2	1	2	4	4	4	0	0	1	52
P4:Efficient Search and Detection	2	4	0	1	0	2	1	1	1	2	4	2	0	1	0	1	0	40
P5:Quick response	4	4	0	1	0	4	1	1	1	2	2	0	1	4	1	1	2	100
P6:Targetted attack defense	4	4	1	2	0	2	0	1	1	1	2	1	1	2	1	1	1	84
P7:Protect LANs from remote cyber attaks	2	4	4	2	0	4	1	2	4	1	4	2	4	0	1	1	4	76
P8:Knowledge gap	4	4	4	1	2	4	2	2	2	0	2	2	1	2	1	0	0	116
P9:Dilever alarm notifications to the CSS SIEM system	2	4	1	0	2	1	1	0	2	0	2	4	1	0	0	0	0	36
P10:Monitor the operability of internal elements	2	4	1	1	0	4	2	2	2	4	4	4	4	4	1	2	1	80
P11:Registeration of security events	2	4	2	2	0	1	0	2	1	0	4	2	2	1	0	1	1	46
P12:Encryption of externally transfered data	4	4	1	0	0	4	1	0	0	0	4	1	0	1	1	1	0	72
P13:CSS must collect,aggregate and exchange security information with each other within stipulated time constraints	2	2	4	4	0	2	0	1	1	1	4	2	2	2	0	1	1	54
P14:Exchanging alarms between CSS centers	2	4	1	0	0	2	1	2	0	0	4	4	1	2	0	2	0	46
P15:Mutually monitoring of operability	1	4	4	1	1	1	1	2	1	4	4	2	2	4	2	1	0	34
P16: Substation resources must have secure access through a centrally supervised gateway	4	4	2	4	0	2	0	2	4	2	4	1	1	2	0	2	1	124
P17: SCADA commands tansmitted over an engineering maintainance interface must be monitored and alarms genrated	2	1	2	0	1	0	4	0	0	0	2	4	1	2	2	1	1	42
P18:Mandatory access control for all devices accessed by engineering maintainance	4	4	0	1	0	1	0	2	1	0	4	4	0	2	1	0	2	88

GAPS IN PRODUCT FEATURES

Product feature	Current state	Where we want it to be
P16: Substation resources must have secure access through a centrally supervised gateway	Inadequately managed, designed, or implemented critical support infrastructure	Additional layers for engineering access channel protection are feasible; these could be achieved via monitored,virtualized access nodes instead of direct connections to substation equipment.
		Digitalized technology can continuously monitor critical functions of high and medium voltage switchgear as well as substation transformers, while performing real-time simulation and diagnostics
P8: Knowledge gap	Inadequate policies, procedures, and culture that govern control system security	Product Education investments and Incorporating education institute to help design capacity building program and cerificates for personal
	Lack of technical training leading to inappropriate command and control system and assets	
P2: Backup and disaster recovery	No advanced, robust, system-level thinking and sense of urgency to mitigate the impact of a major cyber attack	Locolazation of hardware manufactuing and reduce reliance the U.S. energy industry has on imports from China
		Data Back up in multiple locating and develop live disaster recovery plan
P5: Quick response	Insufficiant application of tools to detect and report on inappropriate activity	Incorporation of smart grid or AI to detect and metigate cyber securtiy attacks
		Compile data breach notification laws and scrutinise third party services. Form and train incidence response teams
P18:Mandatory access control for all devices accessed by engineering maintenance	Inappropriate applications or devices on control system networks	Limit user authorization base on sensitivity of information
		Change/Upgrade devices being accessed to be efficiently protected by latest software
P6: Targeted attack defense	Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms	Advanced protection against targeted attacks Network monitoring Threat intelligence Network traffic analysis (NTA) Security Information and Event Management (SIEM)
		Targeted Threat Protection with advanced persistent threat detection and real-time defense against advanced threats.

TECHNOLOGY MIND MAP



TECHNOLOGY

Technology group	Technology	Definition
AI	T1 Behavioral Analytics	use behavioral analytics platforms to find potential threats and vulnerabilities
	T2 Defensive Artificial Intelligence	use defensive AI to detect and stop offensive AI from measuring, testing, and learning how the system or network functions.
	T3 Blockchain	use blockchain to secure systems or devices, create standard security protocols, and make it almost impossible for hackers to penetrate databases.
	T4 Context-Aware Security	reduces the chance of denying entry to an authorized user., context-aware security uses various supportive information.
Software	T5 Network security monitoring tools	used to analyze network data and detect network-based threats.
	T6 Encryption	Encryption protects data by scrambling text so that it is unreadable to unauthorized users.
	T7 Antivirus software	This software is designed to find viruses and other harmful malware.
	T8 Firewalls	acting as an intermediary between your internal network and outside traffic.
Hardware	T9 SCADA hardware firewalls	hardware-based firewalls that provide defense by observing abnormal behavior on a device within the control network
	T10 Integrated circuits	integrated circuit that provides cryptographic functions for protecting the hardware from security vulnerabilities.
	T11 Encrypted Flash Storage	Encrypted flash drives
	T12 Hardware Network Filters	functions as a device on users' home networks, and scrambles traffic packets from trackers.

PRODUCT AND TECHNOLOGY QFD

Product Feature / Technology	Weight	P1:Threat intelligence	P2:Backup and disaster recovery	P3:Penetration testing	P4:Efficient Search and Detection	P5:Quick response	P6:Targetted attack defense	P7:Protect LANs from remote cyber attaks	P9:Dilever alarm notifications to the CSS SIEM system	P10:Monitor the operability of internal elements	P11:Registeration of security events	P12:Encryption of externally transfered data	P13:CSS must collect aggregate and exchange security information	P14:Exchanging alarms between CSS centers	P15:Mutually monitoring of operability	P16:Substation resources must have secure access through a centrally supervised gateway	P17:SCADA commands tansmitted over an engineering maintainance interface must be monitored	P18:Mandatory access control	Total
T1 Behavioral Analytics	2	4	0	2	2	1	4	2	1	0	2	2	2	1	2	2	1	1	50
T2 Defensive Artificial Intelligence	4	4	1	4	2	1	4	2	2	1	2	4	2	0	2	0	2	2	120
T3 Blockchain	4	2	0	4	1	0	4	4	1	0	1	2	1	2	2	0	2	4	112
T4 Context-Aware Security	1	4	0	4	1	4	2	4	2	0	0	1	2	1	1	2	0	2	26
T5 Network security monitoring tools	2	4	4	2	1	0	0	2	2	1	4	4	1	0	2	2	2	1	48
T6 Encryption	4	2	4	1	0	1	4	4	2	0	2	4	4	2	0	0	0	1	100
T7 Antivirus software	4	4	2	2	4	4	2	0	2	1	1	2	0	1	0	0	0	2	84
T8 Firewalls	2	4	2	4	4	4	2	1	0	2	0	0	1	1	2	0	1	0	44
T9 SCADA hardware firewalls	1	2	2	2	0	0	2	4	0	4	1	0	1	2	2	1	2	2	23
T10 Integrated circuits	2	2	4	4	2	4	4	4	0	2	2	1	0	1	2	1	4	2	66
T11 Encrypted Flash Storage	1	0	4	2	1	0	2	4	0	1	0	4	0	0	0	0	2	2	18
T12 Hardware Network Filters	2	2	4	2	0	4	2	2	2	1	0	1	2	1	2	0	1	0	40

GAPS IN TECHNOLOGY

Technology	Feature	Current State	Future State
AI	T2:Defensive Artificial Intelligence	High cost, no ethics or human factor	Low cost, more human input
	T3:Blockchain	Lack of awareness of the technology, internal threat	Raise technology awarness
Software	T6:Encryption	High risk of data loss	Minimize risk of data loss
	T7:Antivirus software	System Slow down	Advanced malware detection
		Limited protection techniques	
Hardware	T10:Integrated circuits	Handle only limited amount of power	Circuits with better capabilites

MODEL OF SYSTEM DEFENSE OPERATIONS/DECISIONS

This model is created to assist the system defender in making decisions. By conducting active defense through a “super-agent” robot and a human, in which the robot can either make an automated judgment or handing off control to the person in the loop (Fig. 1).

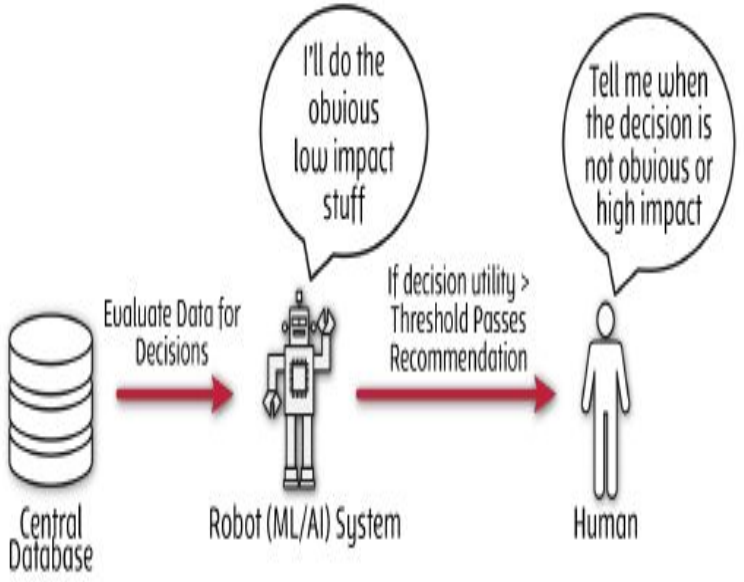


Figure 1 The “Super-Agent”: Robot and Human Cyber-Defense Policy Making

CYBER KILLCHAIN

Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

INFLUENCE DIAGRAM FOR A CYBERSECURITY DEFENDER

An influence diagram is used to illustrate how a decision will be affected by the performance uncertainty of the system's components and their dependencies (here, the defensive response). The defenders' decision-making process is shown as an influence diagram in Figure 3.

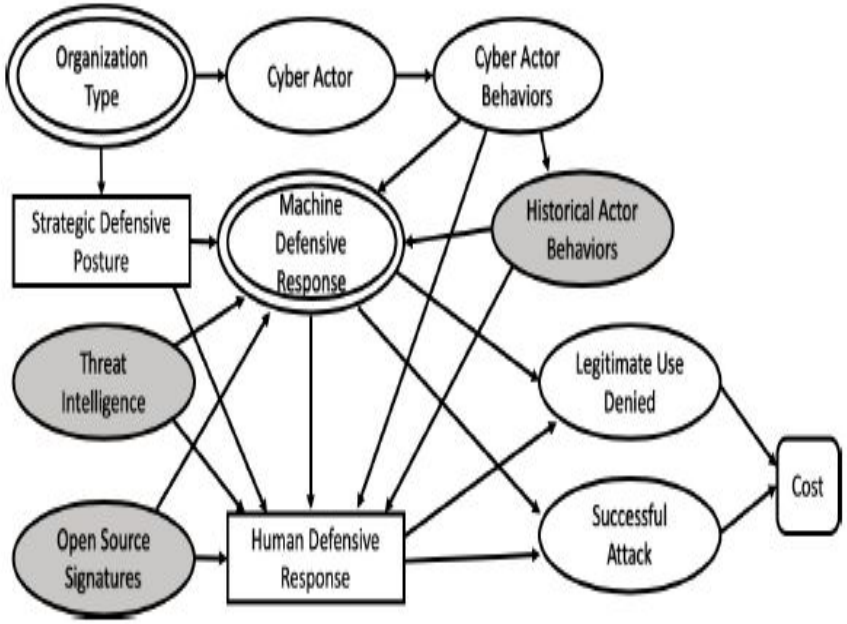
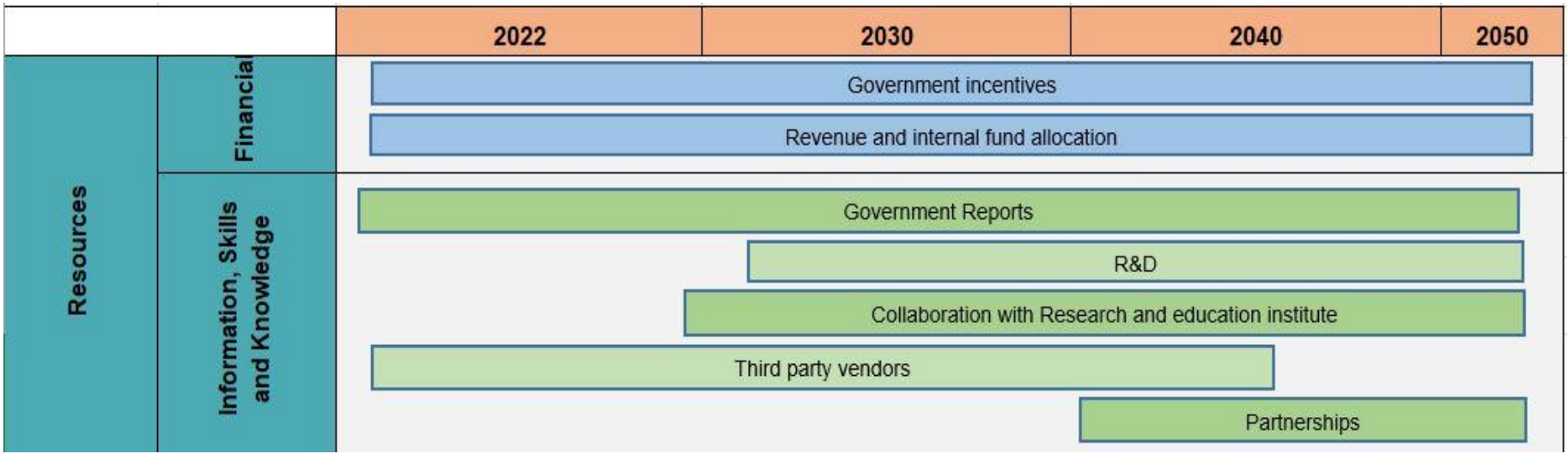


Fig. 3: Influence Diagram for a Cybersecurity Defender

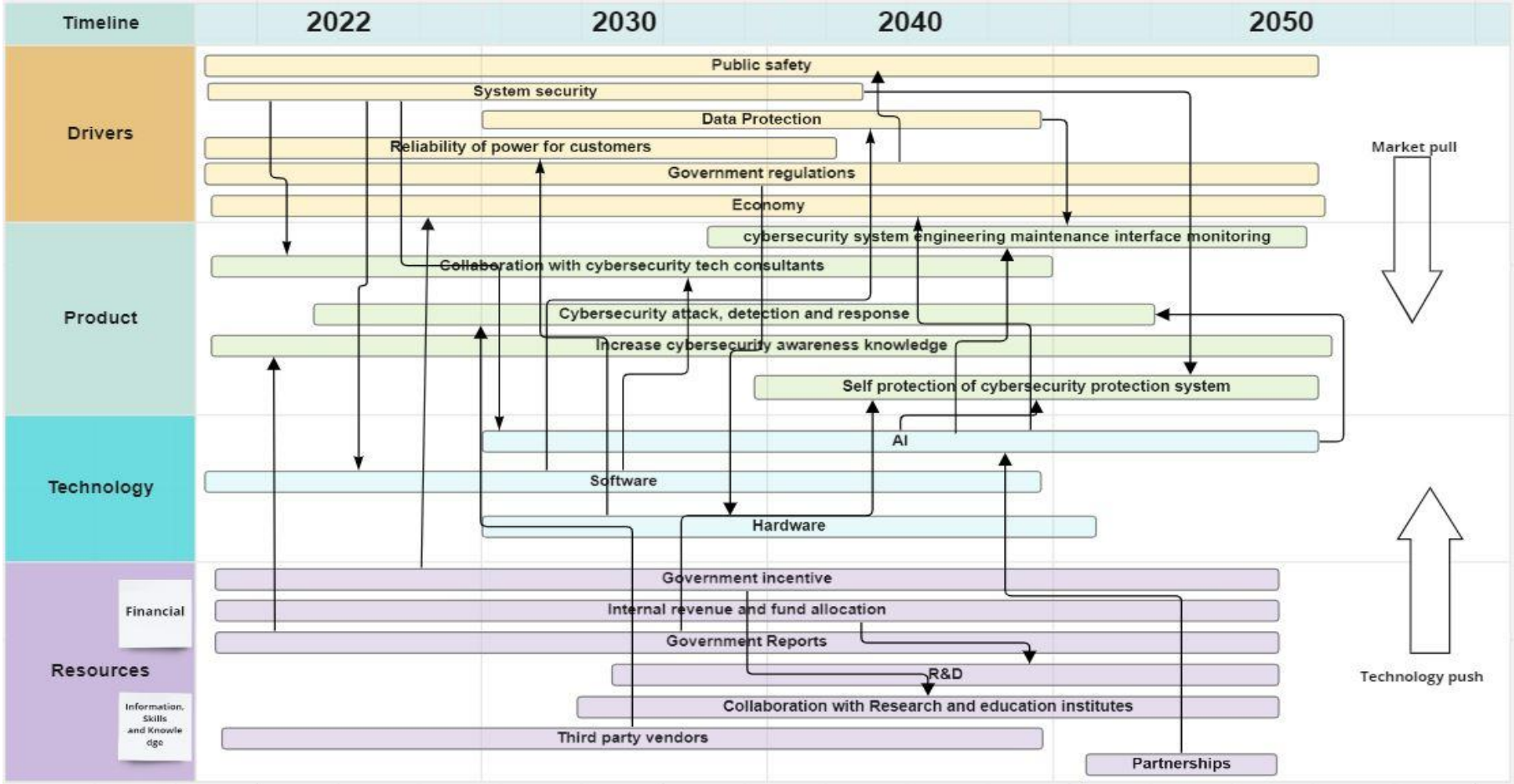
RESOURCES


2022
2030
2040
2050
Resources
Financial
Government incentives
Revenue and internal fund allocation
Information, Skills and Knowledge
Government Reports
R&D
Collaboration with Research and education institute
Third party vendors
Partnerships

RESOURCE ALLOCATION

- Government Incentives : DOE announced April 2022 $12 million for six new research, development, and demonstration
- Revenue and internal fund allocation: funding allocation to for programs training for cyber security team, IT and OT
- Government Reports : DOE NERC FERC reports and assessments about potential attacks and information updates
- R&D: Cyber Security within Research and Development (R&D) Environments To support development and deployment of advanced cyber applications, technologies
- Collaborative with Research and education institute
- Third party vendors.
- Partnership with other providers Cybersecurity, Energy Security, and Emergency Response

ROADMAP


Timeline
2022
2030
2040
2050
Drivers
Public safety
System security
Data Protection
Reliability of power for customers
Government regulations
Economy
Market pull
Product
cybersecurity system engineering maintenance interface monitoring
Collaboration with cybersecurity tech consultants
Cybersecurity attack, detection and response
Increase cybersecurity awareness knowledge
Self protection of cybersecurity protection system
Technology
AI
Software
Hardware
Resources
Financial
Information, Skills and Knowledge
Government incentive
Internal revenue and fund allocation
Government Reports
R&D
Collaboration with Research and education institutes
Third party vendors
Partnerships
Technology push

CONCLUSION

- Cyber physical systems during the cyberattacks can degrade reliability, safety and efficiency. So, Cyber security have become critical priority for PGE.
- As cyber threats can never be fully eliminated but the effect can be minimized, and the impact can be reduced.
- The evolving electricity sector is increasingly dependent on IT and telecommunication infrastructure to ensure the reliability and security and to enhance the products' quality and systems' availability.
- Specific measures to ensure cyber security must be designed and implemented to protect from both cyber and physical attacks by terrorists and hackers, and to strengthen the system against inadvertent threats such as equipment failures and user errors.
- The cyber threat extenuation produces huge spending, exertions, interruption, financial and emotional influences on the business that could affect in destroying the company's performance and the nationwide economies.
- Frequently, digital equipment is connected to the internet to increase the aptitude to share information with a gathering of users and devices.
- Customers benefit from these activities through reducing cyber security related events. They also benefit from the research as PGE continues to focus on securing to ensure that it is reliable and resilient.

REFERENCES

- https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities
- https://mdpi-res.com/d_attachment/electronics/electronics-05-00040/article_deploy/electronics-05-00040.pdf?version=1468499711
- https://assets.ctfassets.net/416ywc1laqmd/2Bv0LaKHnorVeMkLX3Yw7e/329b3f4da35a182b7d24a2a8fc44d4b8/R_D_2020.pdf
- https://www.weforum.org/agenda/2019/04/the-growing-risk-to-our-electricity-grids-and-what-to-do-about-it/
- https://e-tarjome.com/storage/panel/fileuploads/2019-02-24/1551001134_E11831-e-tarjome.pdf
- https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security
- https://www.publicpower.org/policy/grid-security
- https://www.publicpower.org/policy/grid-security
- https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security
- https://abc13.com/ercot-extreme-texas-heat-peak-power-demand-cyber-security-threat/11814751/
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9792263
- https://enroutech.com/cyber-security-services/
- Interview with PGE rep
- https://miro.com/app/board/uXjVOkcRF2U=/?utm_source=notification&utm_medium=email&utm_campaign=daily-updates-variant&utm_content=go-to-board
- international Journal of Critical Infrastructure Protection
- https://arxiv.org/ftp/arxiv/papers/2105/2105.00013.pdf


THANK YOU