INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 10, Issue 1 - V10I1-1240)
Available online at: https://www.ijariit.com

Enhancing Cybersecurity Resilience in a Multinational Semiconductor Organization: A Comprehensive Strategy for Threat Mitigation and Defense Strengthening

Ugochukwu Eneh
ueneh@umd.edu
University of Maryland College Park, Maryland

ABSTRACT

Tososu Semiconductors LLC, a multinational corporation specializing in semiconductor development for medical and automotive sectors, faced numerous cyber threats including ransomware, phishing, and DDOS attacks. This paper presents an in-depth analysis of the attacks experienced by the organization and proposes a comprehensive cybersecurity solution within the constraints of a $600,000 annual budget. The analysis reveals vulnerabilities in the company's network environment, including lack of security awareness among employees, absence of email security systems, and inadequate threat management infrastructure. Subsequently, a multi-faceted solution is proposed to address these vulnerabilities. The proposed solution encompasses the implementation of Unified Threat Management (UTM) systems, human awareness training, backup solutions, DDOS protection, DMZ implementation, password policy enhancement, multi- factor authentication, and phishing detection software. These solutions aim to fortify the organization's security posture, mitigate risks, and prevent future attacks. A detailed breakdown of costs and budget allocation is provided, ensuring adherence to financial constraints while maximizing security measures. Additionally, the paper discusses the implications of the proposed solutions, emphasizing the importance of employee vigilance and continuous security updates. Ultimately, this paper underscores the significance of proactive cybersecurity measures in safeguarding organizational assets and mitigating cyber threats in an evolving technological landscape.

Keywords: *Cybersecurity, Semiconductor Industry, Ransomware, Phishing Attacks, DDOS Attacks, Unified Threat Management (UTM), Human Awareness Training, Backup Solutions, Multi-Factor Authentication, DMZ Implementation, Password Policy, Phishing Detection Software, Budget Allocation, Vulnerability Analysis, Network Security*

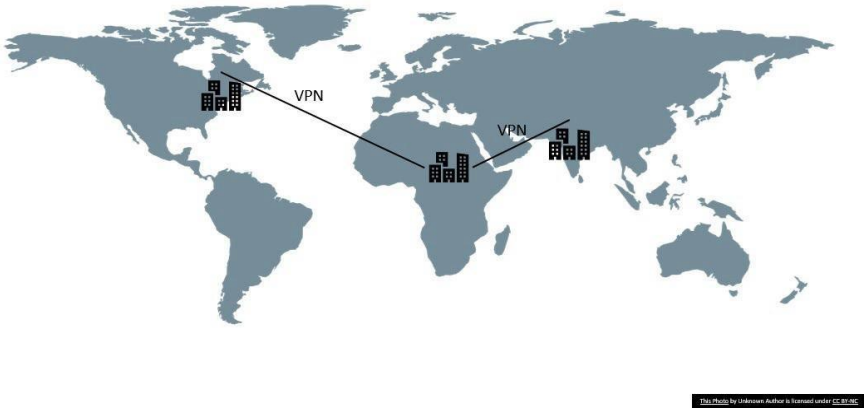
I. OVERVIEW

Tososu Semiconductors LLC is a growing multinational organization that develops semiconductors for medical and automotive devices. It was founded in Washington, DC. Later, the company expanded its offices by establishing research offices in Nigeria and India, which also include the manufacturing and production offices in both locations. The local sales are also done at these research offices, where they have a dedicated sales and billing team to handle the local orders requested by phone or email. Also, both locations have a swarm of Linux systems, forming an individual research network.

The expansion led the office in Washington, DC to become the headquarters of the company focusing on all the administrative work and therefore, forming a Windows Based network. The headquarter office also hosts a webpage for the worldwide clients to check the new products, purchase them and see the progress of their purchases.

Right now, the organization is small-scale and has a workforce of 300 employees across all the current locations. They all operate on the

global ISP network provided by the Expereo Global ISP Provider, which helps them to connect to the internet and helps in forming a single VPN network between the offices with different subnets helping in secure inter-office communications.



II. ANALYSIS

The Attack and the Aftermath

Ransomware Attacks

Being an R&D office, Tososu Semiconductor LLC offices in India and Nigeria already have an internal security team. Over the past 1 year, they have been alerted about multiple ransomware attacks and as soon as the team detected those attacks, they ordered the quarantine of those assets, which prevented the encryption of the whole network. Still, devices that contained important research information were infected and were not recovered. The security team investigated the incidents and reported their findings:

- The ransomware strain was Linux.Encoder.1. It was named by the Russian antivirus firm Dr. Web. It was created to target Linux systems and the first infection was discovered in one of the India office systems. [1]
- The Linux.Encoder.1 virus encrypts all files in the system's home directories, as well as backup folders and system folders connected with websites files, pages, pictures, code libraries, and scripts once it starts infecting the system.
- The ransomware uses the AES encryption, which was used to encrypt all the local files, and only accepts a ransom of $10,000,000 to provide the decryption key but it does not guarantee the key will be provided if the payment is made.
- The attacker(s) gained access to the lab in Nigeria's network by pivoting through the sub-netted VPN while the infected machine was connected to the lab in India's network.
- Since the company was still in the expansion phase, the company had no backup plans which could have been the solution to these attacks.
- The organization decided not to pay because of the absurd amount of the ransom, and therefore, lost all the encrypted data to the attack.
- The machines which were affected by this ransomware were, the Linux storage servers in the India location and two research assistants' research systems in both locations.
- The research office in India was focused on medical-related semiconductors. So, the hit had a major impact on the medical industry because the company followed no backup process.

Phishing Attack

The security team also detected multiple phishing campaigns, where the head researcher and the employee who handles the billing were compromised. The findings were:

- The phishing campaign was a spear-phishing attempt targeting multiple individuals within the organization.
- The attempt was only successful since the head researcher and the employee who handles the billing were not able to recognize the fake email and believed it to be legitimate.
- The email delivered to the researcher was created to make the researcher believe that the email was coming from the IT Department to inform him about the updates made to the IT policies. It required the researcher to log in and read through them.
- But the researcher failed to recognize the email was from a fake sender. As a result, his credentials were compromised.
- The compromise led the attacker to get sensitive information about upcoming changes to the semiconductor.
- The email delivered to the billing department impersonated a local seller of silicon. It stated that there was an update to be made to the account information due to some management changes in their company.
- The employee believed it to be true, changed the accounting information and sent the next order's payment to the hacker's account which resulted in financial loss.

DDOS Attack

The headquarter office, which is in Washington, DC has an external cybersecurity consultant which discovered DDOS attacks that

were targeting the DC office network. The following are their findings:

- The DDOS attack appears to be a volumetric attack, where attackers attempted to create congestion by consuming all the bandwidth between the DC office and the internet.
- The attack appears to be generated using Botnets, which took out the web servers affecting its capabilities to host the client login web app. It took 36 hours to finally regain control.
- This downtime affected the ability of the client to log in and purchase or see the progress on their requests, which in turn affected the sales and the business of the organization.
- After further analysis, the traffic appears to have originated from multiple countries, but the concentration of traffic was majorly from:
    - China – 25%
    - Russia – 17%
    - Malaysia – 6%
    - Ukraine – 3%
    - Indonesia – 2.3%
    - Spain – 1.3%

  And further concentration was distributed evenly but the above traffic appears to stand out in these attacks.

These catalysts observed over the past year, motivated the head of the organization to increase the funding by $600K to revamp the security measures, which is a common trend observed across all the companies. This is not a good practice, and the security of the assets should be a priority from the start, instead of waiting for an attack to introduce these changes.

Assets

Below is the list of operational assets the Tososu Semiconductor LLC has:

- **Research Computers:** The research labs have a total of 60 Linux computers (India and Nigeria). They contain current and future research data and findings and hence are an HVT (high-value target) for attackers.
- **Other Computers**: Some computers are dedicated to employees who are not in the research team but handle the sales, manufacturing, and production. They are on different OS as per the requirement.
- **Administrative Computers:** The remaining computers are in Headquarters, which are dedicated to the administrative work and hosted on Windows OS 7.
- **Employees:** 300 employees are working in all three locations, most of these employees are not up to date with phishing and social engineering techniques.
- **Storage Servers:** There are storage servers at every location hosted on Linux OS that store access, secure, and manage digital data, files, and services related to research, manufacturing, production, employees, and customers.
- **Web Servers:** The headquarters also has web servers used to host the client's login web app.
- **Network Devices:** The local NAS, routers, and switches which make up the intranet need to be tested for firmware vulnerabilities and patched up.
- **Load Balancer -** A load balancer is already installed which helps in distributing the traffic load across the servers running multiple instances of the same application, hence increasing the load tolerance but it failed during the DDOS attack.
- **Perimeter Firewall:** The organization has three layer-2 firewalls, covering the network at each location.
- **Emails –** The organization has the enterprise solution emails from Microsoft and therefore does not maintain email servers as they are managed by Microsoft.

Vulnerabilities in the company's network environment

Following the investigation report from the in-house security team, the outsourced consultant, and scoping the organization's assets, the organization's IT infrastructure has the following vulnerabilities:

- All the offices can communicate via VPN, which also allows users to connect from home but the connection leads to the whole network. Since there is no isolated network, this can lead to an attacker pivoting inside the network, like in the recent attack.
- Lack of security awareness amongst employees means that the employees are susceptible to phishing/ransomware attacks. That also means that the employees may not be aware of the consequences of committing a cyber-crime.
- The organization also does not have any system email security, that can detect phishing emails before even reaching the employee.
- The absence of a threat management system like IPS, IDS, etc. means that there is no filter to block recurring attack attempts. It requires manual interference, which is unreasonably tedious for the security team.
- Also, the organization does not have any central log management system, which can help in providing a central repository for analysis.
- The organization is missing an antivirus solution to protect against known malware, which could have helped in detecting the ransomware.
- The organization does not have a robust password policy, this is evident from the recent breach and needs to be remodeled to make it stricter, but at the same time not too difficult to implement.

- The organization does not have any multi-factor solution to protect its credentials.
- Due to the current expansion phase, the organization is also missing any backup solution, which can provide data integrity and help in providing a quick solution if there is any breach. Also, the company does not have any disaster recovery plan.

Solution Proposal

Solutions

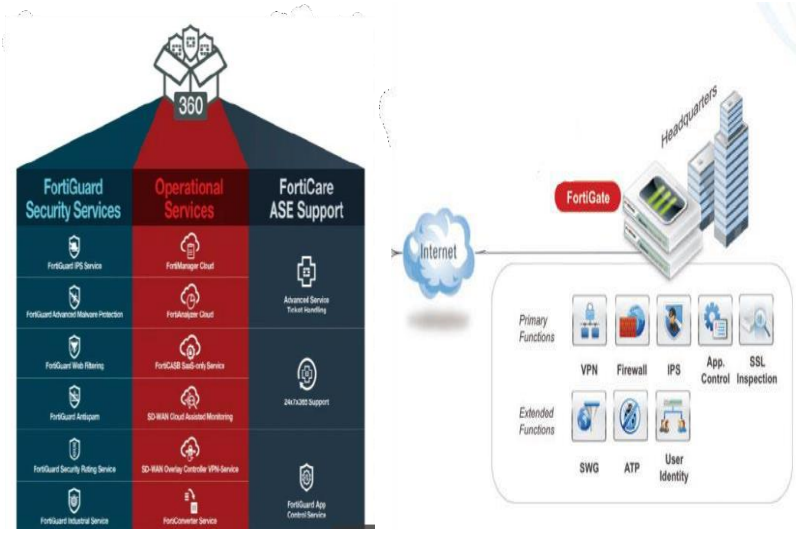
Tososu Semiconductor LLC has had to deal with many threats and attacks as observed for the past 1 year. This means that they must employ many varied solutions to secure their operational infrastructure. It is also important to note that Tososu Semiconductor is a growing organization and one of the constraints is the annual budget limit of $600K which we need to adhere to. As consultants to Tososu semiconductor LLC, we have been hired to help them with steps/techniques that Tososu Semiconductor LLC. should implement to strengthen their infrastructure security and prevents the attacks from happening again:

- **Unified Threat Management system**

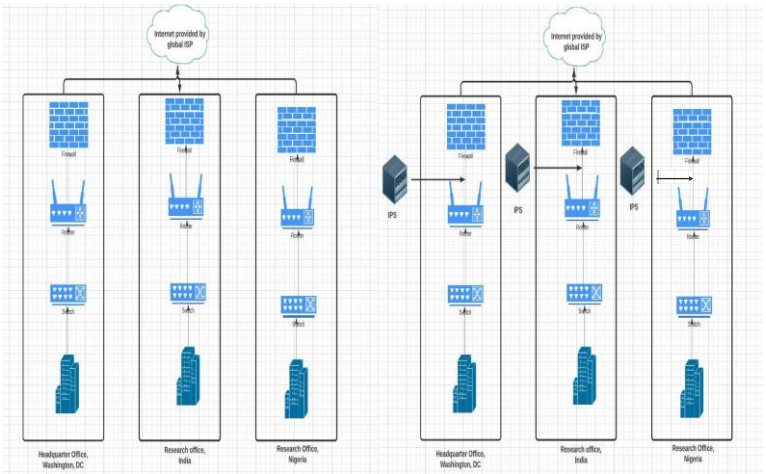
  Implementing security also requires a lot of maintenance, to reduce that, an all-in-one solution would best suit this scenario.

  The FortiGate Enterprise Protection bundle is a comprehensive, cost-effective solution that consolidates the elements of comprehensive protection needed to address the complex threat landscape, today and in the future. It includes a complete set of foundational security services. [2]

  The Enterprise Protection bundle includes essential services such as an intrusion prevention system (IPS), web filtering, antispam, application control, IP reputation services, and monitoring, logging, and reporting.



IPS Services - IPS scans the ingress traffic but does not let the malicious traffic pass through. In the FortiGuard IPS service, the system can detect and take preventative actions like terminating threat sessions and reconfiguring the firewall to prevent such connections from re-establishing. Placing the IPS before the firewall will cause a lot of false positives. Having the traffic pass through the firewall first will ensure that unwanted traffic has already been blocked so the IPS will only have to take action to prevent traffic that passed through the firewall. This will reduce the load on the IPS and make it more efficient.



Advanced Malware Protection – As observed earlier in the vulnerability of the organization, the antivirus solution was missing to protect the endpoints. It could have helped in detecting ransomware which is just malware. FortiGuard Antivirus solution, if purchased will protect Tososu Semiconductor LLC against the latest polymorphing attack components, viruses, spyware, malware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside networks, endpoints, and clouds.

Web Filtering – FortiGuard also provides web filtering services that can protect or limit users' activity on the web. Categories are already specified by the FortiGuard, we can apply a filter based on these categories. It analyzes and scores web pages and if the score is matched, the web page is blocked.

Anti-Spam – This will work in conjunction with any email product. It helps in reducing spam volume at the perimeter, giving unmatched control of email attacks and infections, providing greater protection than standard real-time blacklists, and will be an add-on to security posture.

VPN Protection – FortiGuard also protects VPN connectivity. It supports both secure sockets layer (SSL) and Internet Protocol security (IPsec) VPN. Implementation of IPsec for VPN network will help the labs ensure that the packets of data are protected inside the IPSEC tunnel which helps ensure anonymity by adding a custom IP header.
The split tunneling feature enables remote users on SSL VPNs to access the Internet without their traffic having to pass through the corporate VPN headend, as in a typical SSL VPN tunnel. This feature will reduce latency in the Tososu network, which will improve our users/customers' experience, and provide protection for users working from home. [3]

Central Monitoring, logging, reporting – The organization lacked central log management which could have helped in prioritizing the security alerts and decreasing the remediation time. Implementing FortiGate in Tososu Semiconductor will provide a central platform for logging and reporting which can help in determining what has happened in the network, as well as informing of certain network activity, such as detection of a virus or IPsec VPN tunnel errors from all the above solutions implemented in the network. [4]

Human Awareness Training

Employees must be made aware of the phishing/vishing, social engineering, or ransomware strategies used by attackers. This accomplishes "human firewall", which is a phrase for employees who are knowledgeable about different phishing and social engineering assaults and can defend against them. To achieve this human awareness, training should be organized for all the employees. We will use Cybrary as the platform to provide this training to the employees.

Backup Solutions (Amazon Simple Storage Service (S3))

Tososu Semiconductor LLC. has no backup solution available which affected their ability to restore the data lost during the ransomware attack. We propose implementing cloud backup for Tososu as it is one of the best solutions in which the data and applications on a business's servers are backed up and stored on a remote cloud server. This ensures data integrity and data readiness in the event of a system failure, outage, or natural disaster. Copying data directly to cloud infrastructure providers like Amazon Simple Storage Service (S3) tends to come at a lower storage cost than other backup options. It also provides the following benefits:

- No need for onsite hardware or capital expenses which are well-suited to smaller companies that may outgrow storage too quickly like Tososu Semiconductor LLC. [4]
- The backup or restoration can be performed from anywhere.
- Backup intervals can be set, like 15 minutes, minimizing data losses in disaster situations. Small data set recovery time is improved.

DDOS Protection (Geo Block & DDOS Protection Solution - XCA EDGE)

During the attack analysis, it was observed that there were few countries where the majority of the DDOS traffic was originating. Therefore, one of the temporary solutions to the DDOS attack is to add a geo-block to the countries. Since there is currently no business from these locations, blocking all traffic from these parts of the globe can significantly lower the odds of the infrastructure being hit by attacks which are viable to our small- scale organization and locally oriented websites.

But since it is in the expansion stage and later, we will have to remove the geo-block, therefore, we propose buying an XCA Edge DDOS solution from the global ISP provider Expereo. This will ensure that when an attack is detected, the traffic is redirected to the blackhole center and thus preventing any congestion to the network.

DMZ Solution

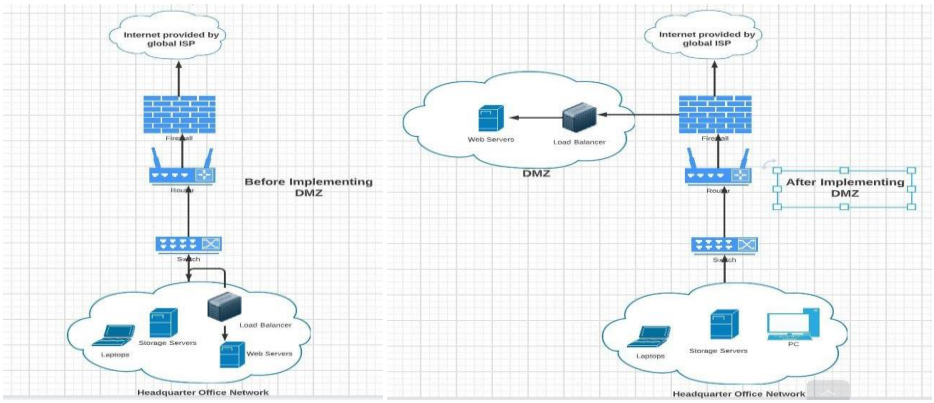
A DMZ is a "demilitarized" zone, implemented by creating a different subnet and placing all the volatile resources like a DNS server, web server, or even a mail server inside that zone. Since we already have a web server at the Headquarter office in DC hosting the web app, this solution can prevent any users on the public internet and restrict their access to internal servers and resources, making it difficult for attackers to access the internal network. There are multiple benefits of using a DMZ:

A DMZ network controls access to services accessible via the internet outside of an

- organization's network perimeters. It also creates a layer of network segmentation, increasing the number of barriers a user must overcome before being granted access to an organization's private network.
- **Network reconnaissance prevention:** In addition, the DMZ prohibits an attacker from scouting possible targets within the

network.

Therefore, if this solution is implemented in the DC office, like below, and later implemented in other locations when any external-facing services are executed. It will help in differentiating the public-facing assets from the main network and thus creating a virtual buffer between the assets and the internet and making it difficult for attackers to access the internal network.



Tososu Semiconductor LLC.

- **Password Policy**
  Currently, the organization does not have a robust password policy, this is evident from the recent breach and needs to be remodeled to make it stricter. Instead of using short complex passwords, we propose the use of passphrases that combine multiple words and are longer than 20 characters and add a policy to rotate the passwords after every 60 days.

- **Multi-factor authentication**
  A robust password policy does not guarantee that employee credentials cannot be leaked and used. Therefore, adding a second authentication system like text messages, or authentication apps adds a second layer of security. For example, in the past when the researcher was phished, and his credentials were leaked. If we had the multifactor solution, the hackers or attackers will not be able to proceed since the second authentication factor was not compromised. Therefore, we propose Duo Factor authentication provided by DUO to add a second layer of authentication for every employee.

- **Phishing Detection Software – Ironscales**
  Phishing is a medium for attackers to enter an organization. It poses a great threat and has a list of negative effects on the organization ranging from loss of money to loss of intellectual property, damage to reputation, and disruption of operational activities. Tososu Semiconductors LLC was affected by the same attack which resulted in the loss of money and compromise of the employee's credentials.

  Human awareness and knowledge sometimes are not sufficient to stop these attacks, therefore, utilizing the phishing detection software can help in preventing the attacks which are too advanced for the employees to detect.
  Ironscales provide the best technique and solution, by approaching emails using an anti-phishing strategy. Below are the most important techniques used for combating and preventing phishing attacks: [6].

  - **Advanced Malware and URL Protection** – Ironscales uses advanced techniques such as deep learning and visual learning so that it can determine if the URL or landing page to which the URL will redirect is suspicious. With this learning, Ironscales dynamically evolve as attackers change their approaches.

  - **API Mailbox-level Intelligence** – Ironscales works from the inside out by building unique profiles for each employee based on communication history, content analysis (NLP), internal, and external relationship profiles, and other metadata. It uses these profiles to detect anomalies or patterns in emails and communications to learn what a bad email or good email looks like and flag suspicious behavior.

  - **Collaborative Threat Hunting –** Ironscales also include decentralized threat intelligence in the report, which leverages the analysis of security teams around the world to help protect against new and evolving attacks. With information, we will be able to anticipate and identify attacks that happen anywhere in the world before they compromise Tososu Semiconductor's mailboxes.

- **AI-Powered Phishing Incident Response –** When phishing incident response comes into play, the manual configuration and deletions are not sufficient. Ironscales also provide incident response systems that will automatically detect and respond to phishing emails in real-time before an employee clicks a phishing email (the average time to click is 82 seconds according to the Verizon DBIR report but Ironscales is faster than 82 seconds).

Solution Analysis

Now we will discuss how the solution, which was proposed will address the vulnerabilities and protect the assets:

S. No.	Solution	Impact
1.	**Unified Threat Management solution** – IPS, web filtering, Anti -Spam & Monitoring, logging, reporting	Improved network scanning and monitoring which will ensure that there is low attack frequency and improved security for Tososu Semiconductor LLC.
2.	**Unified Threat Management solution -** VPN Protection	Improved network anonymity and security along with the smooth operation for the users working from home.
3.	**Unified Threat Management solution - Advanced Malware Protection**	Protection against the latest polymorphing attack components, viruses, spyware, and other content-level threats and continued services to the endpoint which are used while working from home.
4.	**Formation of "Human Firewall"**	Human Firewall will lower the number of phishing and social engineering attacks at Tososu Semiconductor LLC. This will make it almost negligible.
5.	**Backup Solutions (Amazon Simple Storage Service (S3))**	The cloud backup solution will provide easy backup from anywhere along with security. Since it will be backed up every 15 mins, Tososu data set recovery time will be improved and limit the risk of the backups being infected by a malicious program.
6.	**DDOS Protection (Geo Block)**	This solution is only temporary, which will be added to the existing firewall to mitigate the attack and help in decreasing the current load on the bandwidth.
7.	**DDOS Protection (XCA EDGE)**	The solution provided by the global ISP ensures real-time prevention of attacks, where the traffic will be redirected to the blackhole center and thus preventing any congestion to the network.
8.	**DMZ Solution**	The solution will help in differentiating the public- facing assets from the main network and thus creating a virtual buffer between the assets and the internet and making it difficult for attackers to access the internal network of Tososu Semiconductor LLC.
9.	**Stricter password policies that are easy to implement. For example:** • **password length > 20** • **must contain special characters.** • **password should be changed every 60 days.** • **Old passwords cannot be reused**	Credentials authenticate a user to operate a system, having a strong password ensures that attackers must deploy more resources to try to get into the system. Making it strong enough will increase the threshold of resources and profitability threshold.

10.	**Duo – Multi-Factor Authentication Solution**	The solution adds a second layer of authentication which makes it difficult for hackers/attackers to compromise the credentials.
11.	**Phishing Detection Software – Ironscales**	Next-generation anti-phishing software ensures that even if the human firewall fails, the Tososu semiconductor is still in front and up to date against evolving phishing attacks and is acting in real-time.

Budget Breakdown

Tososu Semiconductors LLC. has an annual budget of $600,000 and all the security-related upgrades must be constrained within this budget.

Solutions	Cost (Considering 300 employees combined, in all 3 locations)
The full FortiGuard UTM bundle	$95000/yearly license
Cybrary Human Awareness Training (Ransomware & phishing)	$700 per employee = $210,000
Amazon Simple Storage Service (Amazon S3) (20TB standard storage) [7]	$500 per month = $6000 / yearly
DDOS Protection (Geo Block)	$0
XCA EDGE – Expereo - DDOS protection and mitigation solution.	$3000/month = $36000/yearly
DMZ Solution	$0
Stricter password policies	$0
Duo – Multi-Factor Authentication Solution [9]	$3 per user = $900 per month = $10,800/yearly
IRONSCALES anti-phishing software [8]	$6 per mailbox = $1800 per month = $21,600/yearly
Security Administrator x 2	$100,001 per hire = $200,002/yearly
Total	$579,402

III. CONCLUSIONS

From the high-level overview of the problem statement and the solution proposal, the following inferences can be drawn:

- The organization is a mid-scale one, with over 300 employees in total in 3 locations.
- The security team required a senior security specialist to strengthen the defenses. Hence two new senior security administrators have been appointed in both locations and will help in the transition and installation of the new tools along with training the security team.
- The total budget was 579,402 and $20,598 remaining will be carried over for the next annual budget.
- All the security measures can only provide so much security, employees need to be vigilant and form a strong human firewall.
- Awareness programs will improve our security and make every employee well prepared to fend off any adversaries.
- To stay within the annual budget, we proposed the use of the Unified Threat Management system to supplement the layer 2 firewall Tososu Semiconductor LLC already has because it contains an IPS and other features we believe will improve their security posture.
- If given an additional $250,000 we will purchase:

- Palo Alto Next-Generation Firewall as an upgrade to their Layer 2 firewall.
- A SIEM system for more efficient real-time analysis, monitoring, and alerting on security logs.
- And lastly, we will suggest they hire a third-party penetration testing firm to analyze their whole network for vulnerabilities and evaluate their overall security posture.

- If there was a reduction of $100,000 from our budget. We would propose Tososu Semiconductor LLC. hire a temporary security expert to do in-house training for the employees, instead of using Cybrary.

Finally, it can be said that although security is not a one-time thing, building up new solutions and keeping oneself up to date with all the latest attack vectors will help in better strengthening the security posture of an organization and help defend against adversaries.

IV. REFERENCES

1. https://thehackernews.com/2015/11/linux-ransomware.html
2. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortigate-enterprise-protection- bundle.pdf
3. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/forticlient.pdf
4. https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview
5. https://sysgen.ca/pros-and-cons-of-cloud-vs-in-house-backup/
6. https://ironscales.com/resources/learn/anti-phishing-tools/
7. https://calculator.aws/#/createCalculator/S3
8. https://ironscales.com/pricing
9. https://duo.com/editions-and pricing

