**Project Incident Handling & Risk Analysis**

**Table of Contents**

[**Project Group & Colour Identification 2**](#_8xwiakv2rj4h)

[**Lecture 1 2**](#_xd6lle3cqjwo)

[1} The Tipalti Ransomware Attack 2](#_qrc1uyfmk03b)

[2} Sources 2](#_aun236g1a03d)

[3} Target of the attackers 3](#_ndh5i3oxivq9)

[4} Storage of targeted data 4](#_m6ijyjkgco6s)

[5} Means and type of cyberattack 4](#_ei41xqviyegx)

[6} What interests us about this cyberattack? 4](#_65mci6hn8vc5)

[7} Stakeholder Groups 5](#_xhwbua5uceps)

[8} Cyber attack Incident Report 6](#_ng6uob4rv7fr)

[**Lecture 2 7**](#_hmp7lx49izv7)

[1} Cyber attack incident ENISA threat landscape category 7](#_itp3yjoazb9j)

[2} Stakeholders affected in terms of CIA 7](#_usthl5y5izxc)

[**Lecture 3 9**](#_t4ngitddm3um)

[**Link to NIS Incident Notification Form 9**](#_2khhkcnspjtr)

[**Lecture 4 9**](#_3nmuil61wgwg)

[1} Cyber attack asset identification 9](#_wp6urk10rwpx)

[a) Assets 9](#_ilmd0j3cf6yu)

[b) Explanation of assets 9](#_iin7hnenajrv)

[2} Relationship between stakeholders and cyberattack 11](#_y0j161ln89es)

[3} Stakeholders harmed by cyberattack 12](#_am5t3p5obktx)

[**Lecture 5 13**](#_c0314y67n9uu)

[1} Technique(s) involved in the cyber attack 13](#_sts7986jz9ng)

[2} Prevention and Mitigations with MITRE ATT&CK 14](#_ssa5nj3nq8xl)

[**Lecture 6 15**](#_uqsumfsjh0mi)

[1} Possible exploited vulnerabilities 15](#_m6h1uailyupp)

[2} How much knowledge the attackers had before the attack 16](#_4r65m7rh9mdp)

[3} CORAS projects Links 17](#_rshx8r6mml6n)

[4} Risk Assessments 18](#_uhd2umugnbnt)

[5} Threat Diagrams - More assets attack vectors 18](#_1pvizpkt8byq)

[Lecture 7 18](#_tz1xkpeuco5r)

[1} Working on our threat diagrams 18](#_ksyyjvvxrps6)

[2} Type of Threat Agent involved 18](#_sdcz6iaxuy90)

[**Lecture 8 19**](#_c5drxas31t8a)

[**Lecture 9 20**](#_kt9uktp37qwp)

[**Lecture 10 21**](#_t743eokctex8)

[**Lecture 12 29**](#_fhlqj2g59qfg)

# Project Group & Colour Identification

* **Daniel = blue**
* **Rihards = green**
* **Elvis = orange**
* **Marko = red**
* **FOLOSIYE = purple**
* **Group = black**

# **Lecture 1**

## 1} The Tipalti Ransomware Attack

**Type of Attack**: Ransomware

**Name of company**: Tipalti

**Date of Attack**: 03/12/2023

**Location**: Foster City, California, United states

Tipalti is a software company that provides accounting and software services. It is a payable solution that provides automation software for businesses. It was involved in a ransomware attack on 3rd of december 2023.

## 2} ***Sources***

***Elvis***

**1 -**[***First Link***](https://gridinsoft.com/blogs/tipalti-roblox-twitch-hacked/)

**2 -**[***Second Link***](https://socradar.io/alphv-blackcat-ransomware-attack-on-tipalti-threatening-tipaltis-customers/)

***Peter***

1- [Link 1](https://www.theregister.com/2023/12/05/alphvblackcat_shakes_up_tactics_again/) Jones, C. (n.d.). *BlackCat threatens to directly extort vendor’s customers*. [online] www.theregister.com. Available at: https://www.theregister.com/2023/12/05/alphvblackcat\_shakes\_up\_tactics\_again/ [Accessed 31 Jan. 2024].

2- [Link 2](https://heimdalsecurity.com/blog/tipalti-is-investigating-alleged-ransomware-attack/) Heimdal Security Blog. (2023). *Tipalti Is Investigating Alleged Ransomware Attack*. [online] Available at: https://heimdalsecurity.com/blog/tipalti-is-investigating-alleged-ransomware-attack/ [Accessed 31 Jan. 2024].

***Richie***:

1 - <https://www.bleepingcomputer.com/> (Lawrence, A. (2023))

2 - <https://www.malwarebytes.com/> (Pieter, A.(2023))

***Daniel*:**

1 - [Link 1](https://www.cybersecuritydive.com/news/tipalti-investigates-ransomware-supply-chain-attack/701516/)

2 - [Link 2](https://therecord.media/tipalti-alleged-ransomware-attack)

***Marko***:

1 -Bracken, B.(2023) ’Payments Giant Tipalti: No Ransomware Breach, No Threat to Roblox’, DarkReading, 5 December. Available at: [Link 1](https://www.darkreading.com/application-security/payments-giant-tipalti-no-ransomware-breach-roblox) (Accessed: 31 January 2024)

2 - SOCRadar.(2023) ’ALPHV/BlackCat Ransomware Attack on Tipalti, Threatening Tipalti’s Customers’, SOCRadar, 4 December. Available at: [Link 2](https://socradar.io/alphv-blackcat-ransomware-attack-on-tipalti-threatening-tipaltis-customers/) (Accessed: 31 January 2024)

## **3}** Target of the attackers

The attackers known as ALPHV/BLACKCAT ransomware gang breached Tipalti’s network and stole 256GB of data, including the data from the companies they cooperate with such as Roblox and Twitch.

The group targeted the company's sensitive data that included the information on its employees and customers, the total information BLACKCAT exfiltrated from Tipalti amounted to 256GB of data.

This statement was release by a BLACKCAT spokesperson,

*"Over 265GB+ of confidential business data belonging to the company, as well as its employees and clients has been exfiltrated."*

There was light brought upon the breach early december when

BLACKCAT posted a blog about Tipali on the dark web on the 3rd of december 2023, claiming they have breached Tipalti on the 8th of September “We have remained present, undetected, in multiple Tipali systems since September 8th 2023” - BLACKCAT. This means they remained undetected for several months giving them plenty of time to extract all of the information and prepare the ransome

## 4} Storage of targeted data

Given that the victim and target involved is an accounting software company, it is most likely possible that the stolen and targeted data from customers was saved in a data centre. Big software companies like Google, Facebook and Amazon save their information in massive data centers. Data centres are physical locations where software companies and enterprises that deal with digital products, information and data store computing machines and their related IT systems, such as servers, data storage drives, and network devices. In other words, it is the physical facility that stores any company’s digital data.

## 5} Means and type of cyberattack

Based on research, it is suspected that it was an insider threat work, where an employee or personnel within the company gave access to the cyber group to steal massive amounts of data. An insider threat refers to a cyber attack that originates from within an organisation. It usually occurs when a current or former employee or staff member with certain authentication and authorization access takes actions to damage and fault the organisation's networks, systems, and data.

## 6} What interests us about this cyberattack?

*Daniel* - When researching for a cybercrime attack to discuss, we saw a lot of different cyberattack incidents that caught a lot of our attention and interest. Still, as a group, we decided to settle with the “Tipalti ransomware attack” because it was a incident that involved the theft of massive amounts of data precisely 256 GB of customer information. The data breach was so big that it is expected that as of January 2024, the company will dissolve.

*Peter -* What particularly piques my interest is the attackers involved. The BlackCat Ransomware Gang is a popular Ransom as a service(RAAS) group. They previously attacked Reddit in 2023 and several high-profile universities, and in this Tipalti attack they claim to have accessed information of two of their clients - Roblox and Twitch

*Richie - The cybercriminal organisation known as BlackCat caught my eye whilst I was researching the attack on Tipalti. It took me by surprise to learn the sheer size and power behind this experienced cartel, as they have recorded over 320 attacks on different organisations earning them a place in the most active gangs in the last 12 months.*

*Elvis - While doing research I noticed that the cybercriminals had no real interest in getting a ransom out of the attack. They don't expect the company Tipalti to reach out to them, by going to the policies of the company you can see that they have a policy that removes them from any involvement in a cyberattack. This ransom attack sounds more like an attempt to tarnish the company's image to the public than to get money out of it.-*

*Marko - What Interested me was the tactic that the BlackCat group used. During their reconnaissance attack they noticed that Tipalti didn't want to negotiate with cybercriminals, they also knew that Tipalti didn't have a cyber insurance policy against ransom attacks. Because of that they decided to use extortion on Tipalti’s clients instead of Tipalti themselves.*

## 7} Stakeholder Groups

1. Tipalti Clients & Customers
2. Software companies partnered with Tipalti
3. The Tipalti company (Itself)
4. Others & Non-customers of Tipalti
5. Accounting software companies

## 8} ***Cyber attack Incident Report***

1. Rihards - The damages faced by Tipalti include those of clients losing their loyalty as the security of their data was breached, potentially exposing private information and that of the revenue they will lose due to the decline in customers.
2. Elvis - (*how many users/customers/people were impacted?*)

Based on research, there is no real estimate of the customers impacted by the data breach. All that was stated was that about 256GB of data was leaked and infiltrated by the Blackcat ransomware gang group. The cyber attack was also said to have affected Tipalti’s clients, in Roblox, Twitch, and potentially X (formerly known as Twitter). The stolen data is said to be composed of business data and confidential information of clients and their customers that can potentially threaten Tipalti.

1. Peter - (where in the world were the groups of people impacted)

Since this attack on Tipalti is an accounting data breach involving Roblox and Twitch, it's easy to say the biggest group of people impacted are in the United States of America(USA). To dive deeper at the numbers: as of May 2023 Roblox has 300 monthly users, 70.2 million of them are active daily, and the average Roblox player spends $59.85 on in-game purchases. With the United States-20.21%, Brazil-7.85%, Russia-6.09%, United Kingdom-4.42% and Turkey-4.43%- holding the majority of its users. While for Twitch over 36% of its 94 million users reside in the United States.

1. Marko The attack lasted for 4 days after which the BLACKCAT data-leak website went offline and remained like that for 30 hours. There was rumour that BLACKCAT was the target of a law enforcement operation but there isn’t any evidence to support it.
2. Rihards - Yes there would be an impact on finances, the decline in customers will have a negative impact on the company's wealth, the severity of the impact depends on the scale of the customer's decline. Tipalti’s service offers to “grow your business” for the price of 129 euros a month, a figure not many will be willing to pay after their data breach in early December 2023.
3. Daniel - (*have the attackers been identified/caught?*)

The ransomware gang was identified in ALPHV, also known as Blackcat or Noberus, they are a popular known cyberware gang. They are a ransomware group that has targeted many computer networks, having an estimated 1,000 victims. Their influence has been felt all around the world since the formation of the group, even the U.S. critical infrastructure has had to deal with this particular group. (Link to info on [BlackCat](https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant#:~:text=The%20Justice%20Department%20announced%20today,that%20support%20U.S.%20critical%20infrastructure.))

# **Lecture 2**

## 1} Cyber attack incident ENISA threat landscape category

We believe the attack potentially falls under three ENISA threat landscape categories, These include the obvious Ransomware attack, then the Data breach, and a bit less obvious a Supply chain attack. The full details of the attackers' intentions are still unknown but considering they obtained information about other companies such as Roblox and Twitch could indicate they are also targeting downstream clients.

## 2} Stakeholders affected in terms of CIA

* Tipalti Clients & Customers
* Software companies partnered with Tipalti
* The Tipalti company (Itself)
* Others & Non-customers
* Accounting software companies

C = Confidentiality I = Integrity A = Availability

Rihards - (Software companies partnered with Tipalti)

Software companies that are partnered with Tipalti suffered as they were the victims to the breach in the ‘C’ element in the CIA Triad. Confidentiality, The information of their customers and employees was obtained by this group of hackers and nearly leaked to the public unless a ransom was paid.

Marko - (Tilpati Clients & Customers)

Tipalti clients have suffered in terms of ‘Availability’ after the attack. Tipalti had to shut down parts of their servers for maintenance and to inspect damage caused by attackers, because of this Tipalti customers didn't have access to servers.

Peter - (The Tipalti company)

The data integrity of Tipalti is in jeopardy. Critical data may have been tampered with or altered if the gang has successfully gained access to their systems. Inaccurate financial transactions, unauthorised record modifications, or even the introduction of harmful code into the software could result from integrity breaches.

Elvis - (Others & Non-customers)

Tipalti would lose the trust of its confidentiality to the public, its clients, and future investors of the company, especially with the response of the company itself, investors will believe that the company is not as secure as they were taught to be and will not invest on it because of the fear of their data being stolen.

Daniel - (Accounting Software Companies)

Accounting software companies are affected by the CIA through Availability. Simply because they will be very more inclined to update their cyber and IT security systems, by taking Tipalti as a data breach case example of how an insider threat can dazzle an entire organisation. The software companies will be more likely in a couple of days or weeks to bring down or shutdown their servers and websites for “updating and maintenance” or “patching up bugs” as a means to introduce the new cyber security system against this form of cyber attack/threat. Which will mostly likely and inevitably cut off their clients and customers access to their online services for that short period of time.

# **Lecture 3**

## [Link to NIS Incident Notification Form](https://docs.google.com/document/d/14ffOesD22pqj_i13Gw0UdI8n07_YBdsvuvuq74nWqt0/edit?usp=sharing)

# **Lecture 4**

## 1} Cyber attack asset identification

### Assets

Daniel - 256GB of stolen accounting, vendor and customer data

Elvis - Clients patterns and behaviour

Richie - Cash

Peter - Internal Systems

Marko - Employee data

### Explanation of assets

***Daniel***

The stolen amount of data falls into the information asset type. As it is an asset that was digitally stored and owned by the organisation and individuals. This type of asset is not idiosyncratic to the organisation because it is raw data of its clients, customers and vendors. It would only be idiosyncratic if it is informational data about the organisation itself (e.g. Intellectual property). Customers' data are generally stored and gathered together in similar ways because of their similarities as well. For example, a clients/customers name is stored differently from their date of birth in the database, not necessarily in a different database but certainly in a different format. This asset was compromised because it was an asset that was supposed to be private and confidential, not meant to be seen or collected by the wrong parties. In terms of CIA, its “Confidentiality” was affected and impacted. The stolen data contained private information owned by individuals and organisations that were not supposed to be made public. In reference to sensitivity and criticality, this type of asset is in the category of restricted sensitivity and an essential asset for criticality. It is restricted for sensitivity because it is shouldnt be disclosed or altered by anyone else it would have adverse negative effects on the organisation. It is also an essential asset to the organisation because without it the organisation cannot function or work.

***Elvis***

Customer behaviour, tastes, and purchase trends can all be understood through the use of customer data. Businesses can better understand what customers want by analysing this data, which enables them to design products and services that address their demands. For risk management, having current and accurate customer data is essential. It assists companies in recognizing and reducing any fraud, compliance problems, or other hazards related to their clientele.

Increasing sales and revenue can be achieved by utilising consumer data effectively. Businesses may optimise their offers and pricing strategies by having a thorough understanding of client demands and preferences**.**

***Richie***

*Cash is considered a Current Asset, its* money the company owns or receives from its operations. Cash is not an idiosyncratic asset as its not distinct to the organisation, it is considered a general asset. The impact on the company's cash balance is yet unknown although it was definitely compromised and put in a vulnerable position as the threat actors threatened to leak customer and employee information if a certain cash amount was not met. I would characterise tipaltis business as High Criticality and sensitivity when it comes to this asset because for businesses that rely on accurate payments processes such as a subscription in a digital market, the smooth operations of services is essential as failure to manage payments can result in disruptions to operations and could potentially damage relationships with suppliers and partners.

***Peter***

The asset Internal Systems, which is an intangible asset which would support various business functions (Customer services, human resources etc). Internal Systems is an idiosyncratic to the organisation, as they are unique and made to meet specific needs and operations. In this attack the ransomware group claimed to have managed consistent access to multiple Tipalti systems since the 8th of September 2023 (Cybersecurity Dive. (n.d.). Payments processor Tipalti investigating ransomware attack. [online] Available at: https://www.cybersecuritydive.com/news/tipalti-investigates-ransomware-supply-chain-attack/701516/ [Accessed 29 Feb. 2024].)

This was reportedly done through insider involvement and by these the data exfiltration took place.

Internal systems should be classified as highly sensitive as it will often contain highly sensitive data(e.g customer information, financial data etc)

***Marko***

Employee data is considered an information asset type because it is a collection of data that is valuable to the organisation. This asset is not idiosyncratic because all organisations must have data about their employees. Compromise in security didn’t affect employee data because attackers were focused on collecting and extracting customer data from the servers. There might have been employees who are also customers of Tipalti that would have their data compromised but that would have been their personal data. Even if employee data wasn’t affected by the attack, I would characterise the criticality of this asset as confidential data and sensitivity as high sensitivity data.

## 2} Relationship between stakeholders and cyberattack

The stakeholders identified in the previous lectures are directly related to the assets. For example, the stolen data taken and accessed by the ransomware attack gang was a massive amount of informational data that belonged both by the clients, customers and vendors of Tipalti. So as stakeholders that work hand in hand with Tipalti, it is safe to assume that a part of information from your organisation was accessed or stolen through the attack. A case example are clients like Roblox, X and Twitch who at the time of the cyber attack were working and partnered with Tipalti.

## 3} Stakeholders harmed by cyberattack

Daniel - (256GB of stolen data)

The stakeholder groups affected by the attack on the stolen data are quite many. Stakeholders like customers, clients, the Tipalti organisation (including all employees and workers), vendors, companies partnered with Tipalti whose data was stolen even if partly and others. They are all affected because the stolen data was their private and confidential information. The worst that could happen to the stakeholders depends on the kind of information they owned that was stolen by the ransomware gang group. For example, if a customer’s bank information was stolen then their funds can be accessed and stolen as well. If a partnered software company's secret software was stolen or information of it was shared, it can be sold in the market to their competitors and also for the employees and the Tipalti company itself, it loses the trust of its customers as well as the value of its stock or market value drops.

Elvis - The trust of customers may be damaged by a cybersecurity compromise brought on by a lack of cooperation. Consumers expect companies to protect their data, and any breach can cause confidence to be lost and be hard to get back. The reputation of a firm is directly impacted by the interaction that stakeholders have with cybersecurity procedures. A damaged reputation may result in a drop in total brand value as well as in client acquisition and retention.

Peter - The stakeholders affected by breach of internal systems would be a significant number, the investors who could suffer financial losses from the decreased stock value, customers may potentially suffer reputational damage due to their personal or financial information being compromised, Employees, organisation itself would be tarnished in turn leading to the other stakeholders to lose trust , regulatory bodies would impose fines or penalties, partners and suppliers.

Richie - The compromisation of my asset (cash) would not directly impact the stakeholder groups as the financial damage would mainly be taken by Tiplati as it was their side that was compromised, Although the worst that could happen is that the stakeholders would need to chip in and help Tipalti pay off the ransom if the amount exceeded Tipalti’s budget. The stakeholders would be inclined to help Tipalti as it is their information on the line as well.

Marko - (Employee data)

Stakeholders who were impacted by a security breach of my asset would be the Tipalti themselves and their employees. Employee information, which could contain personal information, was accessed by the attackers which gives them more potential victims to ransom their data to. Employees would lose trust in the company and leave because they cannot keep their personal data secure. Worst case scenario is that attackers use stolen employee data to blackmail the employee to give them access to the Tipalti servers again in exchange of returning their data.

# **Lecture 5**

## 1} Technique(s) involved in the cyber attack

Allegedly, BLACKCAT ransomware group used the **Process Injection** technique to place themselves into Tipalti’s system and remain undetected for several months. In early September BLACKCAT inserted a piece of malicious code into Tipalti’s network and used their trusted legitimate processes (cmd.exe) as cover to mask their malicious activities and avoid basic detection systems.

They likely used Hardcoded Targeting to target Tipalties data management framework

## 2} Prevention and Mitigations with MITRE ATT&CK

Rihards - Tipalti could have implemented Network Segmentation (T1043), to segment the network further to isolate data assets. Tipalti also could have used File Integrity Monitoring(FIM) to scan for IOCs on the systems which would help minimise the chance of Process injection being successful. If the assets remained secure then there would’ve been no need to pay the ransom hence saving their cash assets.

REFERENCE : (MITRE.(nd). MITRE ATTACK. https://attack.mitre.org/)

Daniel - Tipalti’s organisation could have mitigated and prevented the attack by using some of the defence tools in the MITRE matrix. A good example of an enterprise mitigation they could have adopted is M1047 Audit, which involves performing scans of systems, permissions, insecure software & configurations to identify potential weaknesses or holes in the security systems. Another good example is M1040 Behaviour Prevention on Endpoint which observes and prevents any suspicious behaviour pattern in endpoint systems. M1040 would have been especially effective to mitigate the attack as BlackCat masked their malicious activities by hiding behind trusted execution by Tipalti.

Reference : <https://attack.mitre.org/mitigations/enterprise/>

Peter - Tipalti’s organisation could have mitigated and prevented the attack by using the M1017(user Training).Employees may require additional training in some areas to detect and react to phishing attempts, social engineering techniques, and suspicious actions. These areas can be found through routine audits of user security awareness and training programmes. [Reference](https://attack.mitre.org/mitigations/M1017/)

Marko - Tipalti could create an audit(M0947) system which would check the integrity of the system and would help identify any weakness in it. This would have decreased the possibility of security breach because the system would be checked often and any malicious content would be removed from the system.

Reference: <https://attack.mitre.org/mitigations/M0947/>

Elvis - Tipalti could have used the M1037(Filter Network traffic) to filter the ingress and egress traffic and perform protocol based filtering. This would have prevented remote access to the network from BlackCat as well as monitoring the network traffic regularly to prevent breaches.[Reference](https://attack.mitre.org/mitigations/M1037/)

# **Lecture 6**

## 1} Possible exploited vulnerabilities

**Richie-** A vulnerability that could’ve been exploited is the download of code without an integrity check CWE-494. This weakness is caused by a missing security measure that wasn’t implemented during the design phase of the program. This vulnerability could’ve led to malicious code being installed within Tipaltis programs, perhaps code that hacked into their data systems and retrieved all of the customer and employee data which BLACKCAT holds ransoms against tipalti.

Marko - Attacker could have exploited Improper Privilege Management (CWE-269) vulnerability. This vulnerability allows the attacker to change their status from local user to highest level user on the network. Local low privileged attacker could elevate their status to admin level in the targeted system and run commands that would give them unrestricted access to all data in the system.

Daniel - A probable vulnerability the attackers took advantage of is CWE-285 Improper Authorization. As they had access to the system without being authenticated and were able to monitor the system without being detected. It was allegedly said that it was an insider job so the chances of a malicious executable being able to bypass Tipalti’s security system to give them access for surveillance and monitoring are nowhere slim.

Peter- The attackers could have used the Server-Side Request Forgery(SSFR) which is the CWE-918. Commonly internal systems are protected by firewalls or other access controls. This technique can allow attackers to bypass these protections through the requests appearing from trusted servers(that would be tipalti). This would lead to the Backend services,Internal APIs,Backend interfaces ETC to be exposed these are not meant to be accessible from the outside

Elvis - The vulnerability the attackers probably could have exploited is the CWE-863 (Incorrect Authorization). When a user is able to access assets that they shouldn't have access too.

Users can access data or carry out operations they shouldn't be permitted to carry out when access control checks are implemented wrongly. Numerous issues, such as information exposures, denial of service, and arbitrary code execution, may result from this.

## 2} How much knowledge the attackers had before the attack

Daniel - Apparently given the duration of the attack (3-4 months) it is safe to presume that the attackers had some knowledge on their target but it was not enough to conduct an immediate attack. So, with the little access they had to the target system they slowly gathered both information on where to attack as well as the locations of the valued customer and company asset and data.

Marko - Attackers themselves said that they had managed to establish their presence in the Tipalti servers since September 8th 2023. That gave them about 2 months to do recon on Tipalti servers and find the data that they could use when they launched their attack.

Peter - I believe the ransomware group would be quite knowledgeable, as they are very experienced and they targeted Tipalti which are known for their high profile clients such as Roblox and Twitch. They would have gone through thorough reconnaissance. Another reason would be the data that was claimed to be exfiltrated, they would have had the technical prowess to extract a significant amount of data (256GB) without immediate detection. [Reference](https://www.bleepingcomputer.com/news/security/tipalti-investigates-claims-of-data-stolen-in-ransomware-attack/)

Elvis - The attackers meticulously planned their assault on Tipalti, investing ample time in research and reconnaissance. Such sophisticated attacks don't materialise overnight; they require careful planning and a deep understanding of the target. Delving into Tipalti's operations, they gathered extensive information on their clients, studying their patterns, vulnerabilities, and potential points of entry. With a clear goal in mind, the attackers strategized on how to exploit Tipalti's systems effectively. They identified weaknesses in the infrastructure, loopholes in security protocols, and potential avenues for infiltration. Through thorough analysis and probing, they crafted a comprehensive plan of attack, aiming to breach Tipalti's defences and achieve their objectives.

Rihards - BLACKCAT was established in 2021 and since then they have launched over 100 coordinated attacks which involved data leaks. We are obviously dealing with professionals, and they wouldn't begin an operation of this scale blind. I think they had a lot of knowledge prior to the attack, as in the past BlackCat relied on stolen credentials that they obtained through Initial access brokers. I think they exploited this vulnerability to gather as much information about the company and its employees before launching the attack.

## 3} CORAS projects Links

Daniel - Coras Project link

Marko - [Coras link](https://setuo365-my.sharepoint.com/:u:/g/personal/c00281260_setu_ie/EU1VrhYcRf1DhjSWa6QhMIsB3_wVzu8aNAgOYRgyRzQiww?e=5LYh7M)

Richie

Peter

Elvis

## 4} Risk Assessments

Marko -

C - Attackers exploit the use of default login credentials to gain access to servers and download employee data.

I - Attackers exploit improper privilege management in the network to gain higher privilege and modify or delete the employee data.

A - Attackers use DOS attacks on the network to block access to employee data.

## 5} Threat Diagrams - More assets attack vectors

Richie - Cash Asset

# **Lecture 7**

## 1} *Working on our threat diagrams*

## 2} Type of Threat Agent involved

A threat agent is a subject that produces and brings about a threat to a person, group or organisation. In our cyberattack with Tipalti, the threat agent can be divided into 2 as it is not certain which came after the other or if both actually occurred as opposed to one. The threat agent is initially external as a breach was committed by a cyber ransomware group known as the ALPHV or BlackCat. And the other is internal as it was reported that it was an insider job. Details on the type of insider job it was as not been disclosed, so it cannot be ascertained if it was accidental or intentional. Though we presume, the threat agent is more likely to be external as the hacker group monitored and surveilled the organisation’s data movements unnoticed and unbeknownst to them. The threat action used by the attackers was a system intrusion attack which allowed them to deploy their ransomware and put them in a dominant position when demanding money.

# **Lecture 8**

1}

One of the assets our team is responsible for is data. The route the attacker took to compromise Tipaltis data asset would involve the attacker firstly having a degree of knowledge about Tipalti’s organisation.

Rihards - I think Information disclosure was the category utilized to carry out the attack as in the end the information that was disclosed got put up on the line by the threat actors and gave them leverage to demand money from tipalti. The MITRE ATT&CK Tactic used was Exfiltration, specifically I think it was Exfiltration over an existing command or control channel. BLACKCAT remained undetected for several months before revealing their presence. During their time in Tipalti’s network they were extracting information and like I mentioned before I think they used those channels by encoding the stolen data into the normal communications channels using the same protocol as command and communications

2}

Rihards - Tipalti has security measures in place and regular monitoring of the network. I think the likelihood would be a 3 (Possible) and although the compromise of the data repository would have high consequences, I don't think it would result in catastrophic failure of the entire organisation so I think the impact would be 4 (severe). I think it would still be on the high end as the attack tipalti were subjected to had an impact on shareholders and their information as well. This could damage trust between the companies and weaken Tipalti’s organisation.

With these measures calculated, the Risk is determined by Multiplying the Likelihood and Impact measures (3x4) which gives us a risk of 12. This is considered as Medium High.

I don't think the risk calculated here can be compared to the NVD level as NVD risk level focuses on vulnerabilities and threats rather than individual assets such as the one I calculated here.

# **Lecture 9**

1}

Threat model diagram [Link](https://setuo365-my.sharepoint.com/personal/c00281260_setu_ie/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fc00281260%5Fsetu%5Fie%2FDocuments%2FSample%5FThreat%5FModel%2Etm7&parent=%2Fpersonal%2Fc00281260%5Fsetu%5Fie%2FDocuments)

2}

**Daniel**

* **Weak access control for a resource**
* **Data flow generic data flow is potentially interrupted**
* **Elevation by changing the execution flow in OS process**
* **Spoofing the OS process process (Rough Notes)**

**Rihards**

* **I think the sector I would need to focus on would be the Data Stores. If a threat actor would gain access to this sector my asset (cash) could be compromised. I would need to address the threat of Information Disclosure. I would do this by firstly implementing a preventive control such as encryption so the data would need a decryption key to access it. I would also implement a detective control such as an Intrusion detection system so I can monitor network traffic and detect any potential threats. I would also put administrative controls in place such as supervision of personnel to ensure policies and procedures are being followed and lastly I would add a corrective control such as an incident response plan so the attack can be contained and then eradicated.**
* **I would also propose using Input and processing controls, the input control would ensure the input is accurate and is audited and the processing control would compare records to catch errors in real-time so reports of any suspicious activities will be instant and can be addressed and contained.**

**Peter -**

# **Lecture 10**

1} Cost of protecting the assets

1.

Rihards - A control I would implement to protect my asset (cash) would be Security awareness training, this should help the organisation minimise the chances of being the victim to a ransomware attack.

Reference;

“Phished.io” May 5, 2024. https://phished.io/.

A} To implement this control to a small to medium company it would cost a minimum of $145/month which would equate to 1750 per annum at the cheapest for a full course in security risk awareness that you can do while still maintaining a full-time job. Completion of this course would give the employees a Certificate and also improve their knowledge base for the future. This would be a driving factor in getting the employees on board to attend this course.

B} Before the implementation of this preventative control the organisation would be alot more likely to be vulnerable to a successful attack but with spending the extra money to mitigate the risk and enrol the employees in this course we severely reduce the likelihood of a malicious attack being successful. The course has promised to drastically lower the incident rate in our company

“improve your organisation’s cyber security and obtain a zero incident rate”

According to <https://www.varonis.com>

65% percent of companies experienced at least one ransomware attack in 2023. This means a company is expected to receive at least one attack lets say every 1.5 years.

They also stated that the average ransomware attack in the financial sector was 5.9 Million dollars.

It appears that 60% of ransomware cases, the malware is installed directly onto the desktop by workers, according to Verizon’s 2021 Data Breach Investigation Report. With the correct education and reduced carelessness the massive loss of nearly 6 Million can be reduced by 60% if this preventive control is implemented.

C} Depending which sector your company is operating in the cost of an attack. On average the attack would cost 2 million but can be be reduced by 60 percent on average if this preventative control is implemented.

2.

• Single Loss Expectancy = €2,000,000

• Rate of Occurrence (before control) = 1 per 1.5 years

• Annual Rate of Occurrence (before control) = 0.75

• Annualised Loss Expectancy (before control) = €1,333,333

• Annual Cost of Control = €1,750

• Rate of Occurrence (after control) = 1 per 2.4 years ( 60 percent decrease)

• ARO (after control) = 0.4

• ALE (after control) = €833,333

• ROSI = €1,333,333 – €833,333 – €1,750= €498,250

Daniel - The theft of data in today’s society has become one of the most regular and common things. And to mitigate this issue, many controls were put in place and established in various companies, such as file encryption, 2FA (2-factor factor-authentication), integrated firewalls,etc. But if I were to implement one specific control it would be 2FA as it offers the use of a short term pin, code or password in conjunction with the use of a long-term password.

Link - [How companies protect customer data?](https://www.techtarget.com/searchcustomerexperience/answer/How-do-companies-protect-customer-data)

A} A particular reason why I prefer and advise to use 2FA over other security controls is because it is nearly free, cheap and affordable for most companies. 2FA also comes in various forms, it could be with a short-term code via SMS or call, a link through email, authenticator app or even biometrics where a user’s fingerprint or face scan is required for authentication.

Basic SMS 2FA costs very low and is sometimes even free. It goes for £10 - £15 per user per month or from £30 - £50 for more complex solutions per user per year.

So, for the basic SMS solution in a small-sized company of 100 employees, it would cost between £1000 and £1500 annually, and for a medium-sized company of 250 employees, it would cost between £2500 and £3750 annually. And taking Tipalti as a case example, it has roughly around 3000 users plus maybe 120+ employees. With basic SMS 2FA, the cost would rise to £31,200–£46,800, while with the robust 2FA option, it would be £93,600–£156,000. These prices are little to nothing compared to the fines given to companies that violate GDPR rules and regulations, which soar into the millions.

Link: [Why 2FA is important for business computer security](https://systemforce.co.uk/why-two-factor-authentication-is-important-for-business-computer-security/#:~:text=Generally%2C%202FA%20solutions%20range%20from,can%20involve%20higher%20upfront%20costs.)

B} In percentage terms, what is the likelihood of a cyber threat actor or group of cyber attackers targeting sensitive data from a company? The percentage of sensitive and confidential information and data targeted by cyber threats is between 80% and 95%, meaning that most attacks (not all) start or continue with the sole purpose of getting/stealing private data from customers, businesses and employees. So, we see that even with or without any controls, the frequency of attacks barely reduces but perhaps the success rate of successful attacks drops instead. We see that Tipalti already had 2FA in place when they were successfully attacked. So, my advice would be to use a more robust version of 2FA and that the frequency of successful attacks was low as only one account was recorded, but I want to believe that 5 times a year is suitable to set for cyber attack success frequency before control and 4 times a year after control.

Link: [Tipalti's Financial Fraud Report](https://tipalti.com/en-eu/guide/financial-fraud-report/)

C} A data breach attack on a finance company would approximately cost $6 million dollars in damages. With an average of $1.58 million dollars on average.

Link - [Cost in Damages](https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/#:~:text=Financial%20institutions%20ranked%20second%2C%20with,1.58%20U.S.%20dollars%20on%20average.)

2} Single Loss Expectancy = $6,000,000

Rate of Occurrence (before control) = 5 per 1 year

• Annual Rate of Occurrence (before control) = 5

• Annualized Loss Expectancy (before control) = $6,000,000 x 5 = 30,000,000

• Annual Cost of Control = $156,300 (average of robust 2FA in $)

• Rate of Occurrence (after control) = 4 per 1 year (20% decrease)

• ARO (after control) = 4

• ALE (after control) = $24,000,000

• ROSI = $30,000,000 -$24,000,000 -$156,300 = $5,843,700

Marko – I would implement regular pen testing every few months to ensure that there aren’t any security weak spots in my organisation that could harm my asset.

A} The cost of professional pen testing would be the minimum of $15,000 for a single test. If we had a pen test every 2 months, that would cost at least $90,000 annually. This pen test would ensure that the organisation's security is up-to-date and would discover new vulnerabilities in the security that could be exploited.

Reference: https://www.securitymetrics.com/blog/how-much-does-pentest-cost

B} Company can experience at least a dozen ransomware attacks in a year, but only 7% of all ransomware attacks in a year are successful. I speculate that the company will be successfully attacked once every 4 years before control is implemented and roughly once every 13 years after control is implemented.

C} In 2023, 93% of ransomware attacks didn’t result in any loss or they failed, while the remaining 7% paid on average 568,000 dollars for the attack. By having the pen test every 2 months, we reduce the chance of successful attack, which in turn increases the chance of ransomware not causing any loss to the company.

• Single Loss Expectancy = 568,000$

• Rate of Occurrence (before control) = 1 per 4 years

• Annual Rate of Occurrence (before control) = 0.25

• Annualized Loss Expectancy (before control) = 142,000$

• Annual Cost of Control = $90,000

• Rate of Occurrence (after control) = 1 per 13 years

• ARO (after control) = 0.077

• ALE (after control) = 43,736$

• ROSI = 142,000$ – 43,736$ – 90,000$ = 8,264$

Peter - A control I would implement to protect my asset (internal systems) would be Risk Assessment, This involves the identification and analysis of relevant risks to the achievement of objectives, forming a basis for determining how the risks should be managed.

The cost of adopting a risk assessment control varies substantially based on the organisation's size and complexity, as well as the unique risks involved. Risk assessment usually ranges from $20,000 to $25,000 (Project Risk Management FAQs, n.d.). (Available at: https://www.oregon.gov/odot/Engineering/Docs\_RMVE/Risk-FAQ.pdf.)

‌

It is critical to emphasise that the cost of adopting these controls would be less than the possible loss from a risky event. Poor risk management can cost an organisation its reputation; it would also induce some human cost as Poor risk assessment and finger-pointing also have enormous human costs like lack of trust, anxiety, etc Bilich, T. (n.d.). *The Costs of Poor Risk Assessment | Risk Alternatives*. [online] Available at: <https://riskalts.com/the-costs-of-poor-risk-assessment/>.

B. The frequency of successful assaults before and after control can be reduced greatly by implementing risk assessment controls (ISACA, 2012). However, the actual frequency of attacks before and after installing these controls varies substantially based on each organization's unique circumstances. The NIST Cybersecurity Framework (NIST Cybersecurity Framework 2.0: (2024). doi:<https://doi.org/10.6028/nist.sp.1303.ipd>). offers recommendations for lowering cybersecurity risks and can assist organisations in discussing, organising, and addressing gaps in their cybersecurity programmes in a consistent manner (NIST, 2014).

c. The cost of a cyber incident can be significant, and it is crucial to remember that the cost of implementing controls should be less than the potential loss from a risky event (Ponemon Institute, 2018). Implementing risk assessment controls can significantly reduce the cost of an attack. (CO S ST OF A CYBER INCIDENT: YSTEMATIC REVIEW AND C ROSS-VALIDATION) (2020). Available at: <https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf>.

Elvis - I would choose to implement Detective Control, the Intrusion Detection System. It is designed to provide real-time or almost real-time monitoring and alerting by detecting aberrant behaviour or unwanted access on a device or inside a network.

One of the many options available that I would choose would be SNORT, as SNORT is a potent open-source intrusion detection and prevention system (IDS/IPS) that offers data packet tracking and real-time network traffic analysis. To find possibly malicious activities, SNORT employs a rule-based language that integrates anomaly, protocol, and signature inspection techniques. It is free and available for anyone who wants to use an IDS or IPS to monitor and protect their network.

B)Worldwide, ransomware attacks affected a sizable portion of enterprises in 2023. In particular, around one out of every ten firms worldwide experienced attempted ransomware assaults during the year, a 33% rise from the year before. Furthermore, over 5,200 firms were reportedly hit by ransomware attacks throughout the course of the year, however underreporting certainly added to the true figure. This research emphasises the necessity for strong safety precautions by highlighting the pervasive and growing danger posed by ransomware attacks across numerous sectors.

Source:[Rapid7](https://www.rapid7.com/blog/post/2024/01/12/2023-ransomware-stats-a-look-back-to-plan-ahead/)

C)A successful ransomware attack can have a significant financial impact, with expenses going well beyond the first ransom payment. Excluding the ransom itself, the average recovery cost from a ransomware attack in 2023 was close to $1.82 million. This covers, among other things, costs for reputational harm, downtime, and system repair. Businesses that choose to pay the ransom saw a sharp rise in expenses, which averaged roughly $2.6 million when the ransom was taken into account. According to Varonis AI Security, SC Media, and other sources, the average ransom payment increased dramatically from $812,380 in 2022 to $1,542,333 in 2023.

These figures show the serious financial burden that ransomware can place on businesses, underscoring the need for strong cybersecurity defences and incident response strategies to lessen the risks and possible losses brought on by these kinds of assaults.

Reference:([Varonis AI Security](https://www.varonis.com/blog/ransomware-statistics))​​ ([SC Media](https://www.scmagazine.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023))​​ ([SC Media](https://www.scmagazine.com/resource/key-findings-the-state-of-ransomware-2023-report))​.

Retrospective

Overall, we are happy with the attack we chose, as we’ve put in a lot of work and have grown to understand the attack in detail. It was disappointing that there was no resolution to the Tipalti attack in real life, so we could see if any of us came up with the way they were actually compromised.

# **Lecture 12**

1} The root cause of our incident was the insider threat posed by an employee who gave access to the Tipalti network to the attackers. There are several ways to prevent this security vulnerability from happening again or reduce its impact on the organisation. The first way is to implement a detection program to detect and block users if they try to misuse their privilege. A second way would be to implement multi-factor authentication and train employees in safe password practices to reduce the chance of an insider stealing someone's credentials and using their account for malicious purposes.

2} There have been 142 confirmed ransomware attacks in Q1 2024, but none of them are similar to ours in a way that they used insiders to gain access to the network. However, there were also 939 unconfirmed ransomware attacks in that time period, so there is a possibility that there is a case that is similar to ours, but there isn’t any reliable information about it.

Advice as a security consultant

Layered Security: Use a multi-layered security strategy that encompasses endpoint protection, network security, application security, and data encryption.

B. Improve Incident Detection and Reporting: Increase incident detection capabilities and build reliable, timely reporting systems.

C. Regular Network Scanning: Scan your network devices and software on a regular basis to inventory them. Remove any unneeded or unexpected hardware and software from the network.

D. Secure Transactional Data: Monitor financial workflows to discover and respond to irregularities quickly.