Cybsec by Deloitte.

Attacking Payment Application Development Companies

Julio Ardita – Cybsec by Deloitte - jardita@deloitte.com

Cybsec by Deloitte.

Agenda

1 – Security Incidents

2 – CIR Strategy

3 – Real Experiences

4 - Conclusions

Cybsec by Deloitte.

Agenda

1 – Security Incidents

2 – CIR Strategy

3 – Real Experiences

4 - Conclusions

Cybsec by Deloitte.

Security Incidents

Public vs. private security incidents

- Frauds – Theft of money through email and fake sites.
- Threats and extortion.
- Sabotage and erasure of virtual servers.
- Data theft
- Massive phishing focused on banking frauds / large businesses
- Denial of Service attacks

Cybsec by Deloitte.

Security Incidents

Ransomware – Data seizure

WannaCry – May 12, de 2017

Petya – June 27, 2017

Operating mode

- Phishing
- Exploitation of vulnerabilities
- Data encryption

Cybsec by Deloitte.

Current Trend

- Increase of security incidents.

- Exponential growth in the number of phishing attacks against Argentine financial entities.

- Ransomware attacks (data encryption).

- Hacktivism (**404 Sector in Argentina** and **Anonymous Argentina**).

- Data sources: Open Wifi networks or TOR networks.

Cybsec by Deloitte.

Incidents Management

The question today is not “will I have a security incident”, but:

When will I have it?

Maturity in internal security incident management

- No management (85%)

- Disorganized incident management (8%)

- Formal incident management for appearances sake (compliance) (4%)

- Real, formal incident management (2%)

- Internal CSIRT (<1%)

Cybsec by Deloitte.

Agenda

1 – Security Incidents

2 – CIR Strategy

3 – Real Experiences

4 - Conclusions

Cybsec by Deloitte.

Security incident management

We do everything possible to achieve a high security level in the Organization, but a severe security incident arises.

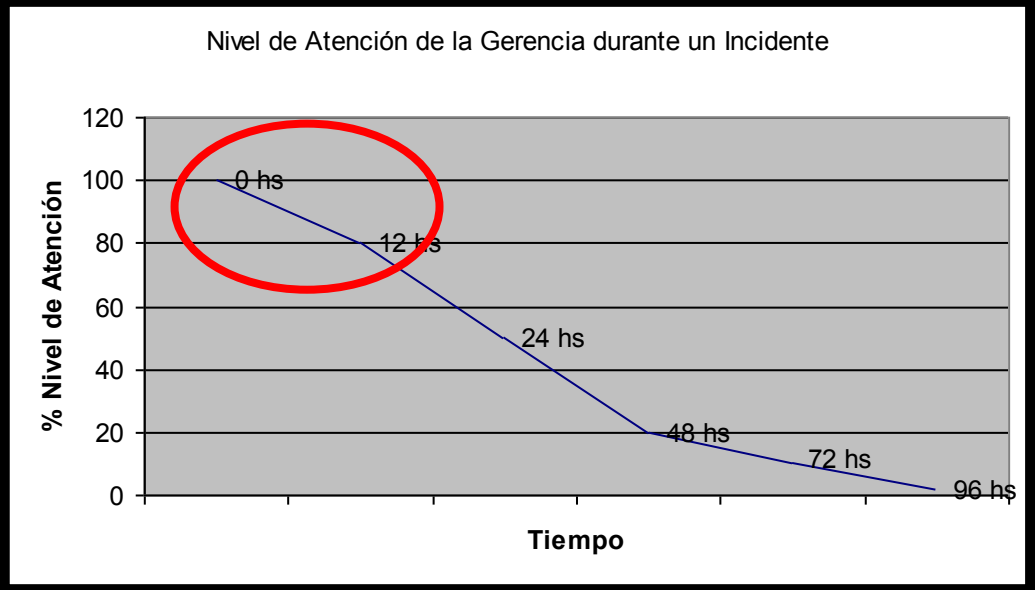
Recommendations:

- Do not hide it.
- Keep calm at the CSO personal situation
- Do not begin by searching for culprits
- Gather first hand information and verify it
- Establish and coordinate an Action Plan

Cybsec by Deloitte.

Security incident management

During the first hours, the Company will be paying attention to us. We must take advantage of this.

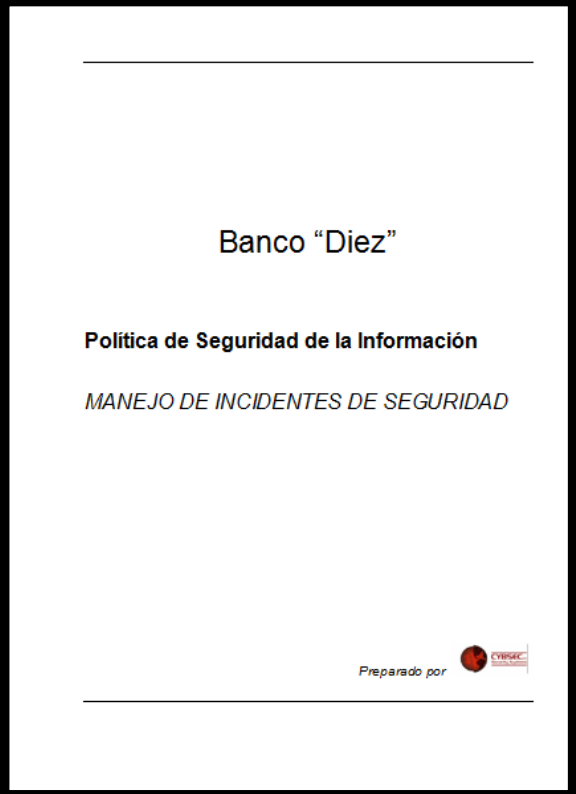


Cybsec by Deloitte.

Information Security Incident Management Policy

Issues to be considered:

1. Detection and notification of Information Security Incidents
2. Information Security Incident Tracking
3. Gathering of proof
4. Recovery process of the affected systems
5. Disciplinary process


Banco "Diez"

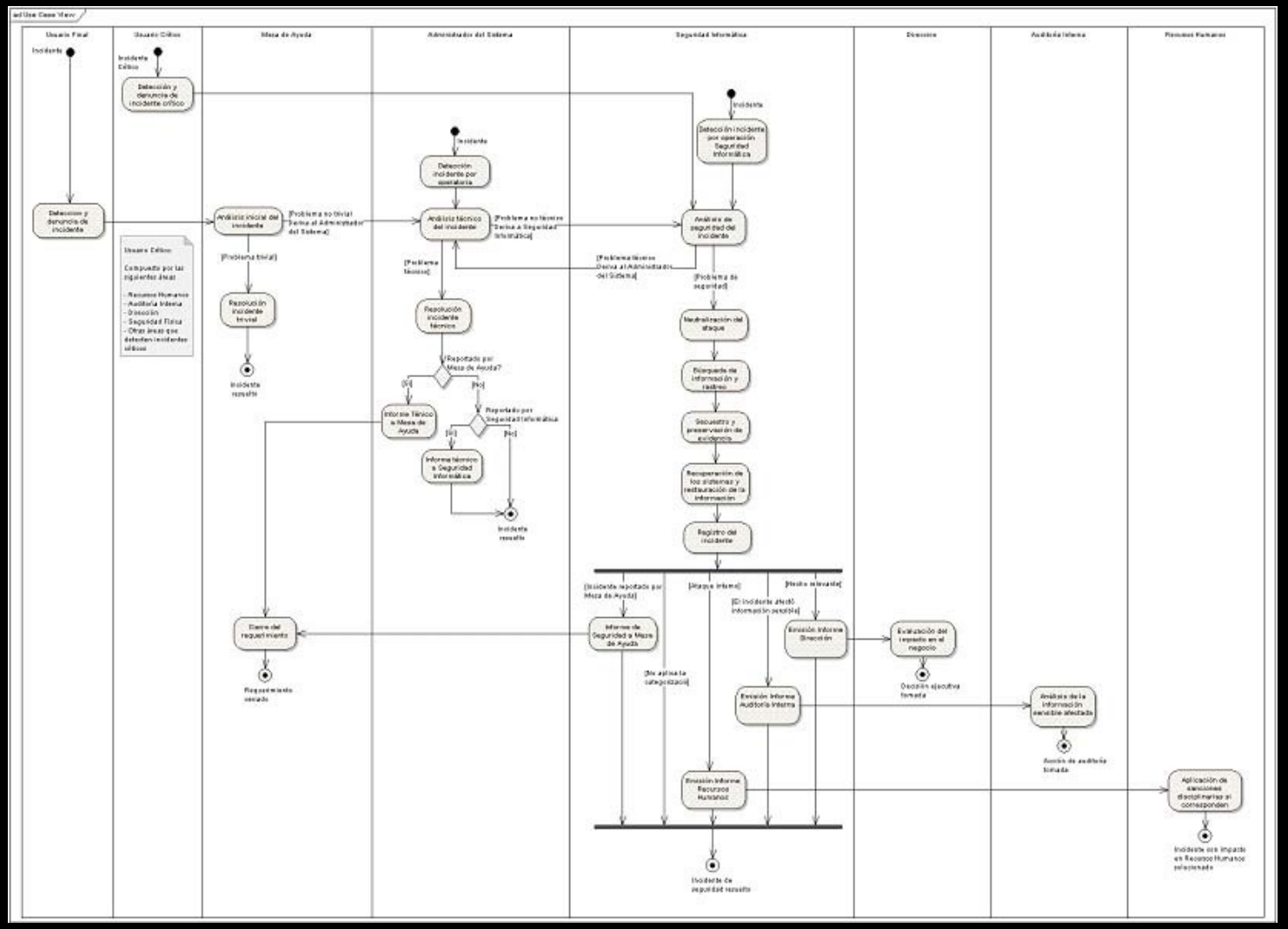
Política de Seguridad de la Información

MANEJO DE INCIDENTES DE SEGURIDAD

Preparado por

Cybsec by Deloitte.

Internal incident management flowchart



Cybsec by Deloitte.

Agenda

1 – Security Incidents

2 – CIR Strategy

3 – Real Experiences

4 - Conclusions

Cybsec by Deloitte.

CASE 1: Theft of batch with credit card data

Incident description:

In April, 2014, we were contacted by a Company that sells tickets over the Internet because the processor that authorized the payments informed them that they were a point of compromise, as they were detecting and recording purchases that were not recognized abroad, and the fraud prevention system showed that all the cards had passed through the same merchant.

A survey meeting was held with the processor and the company involved. They provided us information on the compromised card batches to launch an investigation.

We worked on two lines of investigation:
- Investigate what happened and curb data theft.
- Track the source.

Cybsec by Deloitte.

CASE 1: Theft of batch with credit card data

Research methodology:

1. The type of fraud was researched: in some cases, they involved cloned cards and in others, they were not-present transactions (which meant that they had robbed the following information: PAN, expiry date, security code, Track 1 and Track 2).
2. It was determined which systems contained said information and they were assessed. Two internal systems were detected: the Reserves and the Payment System.
3. Compromised cards were searched for and they were detected in both systems.

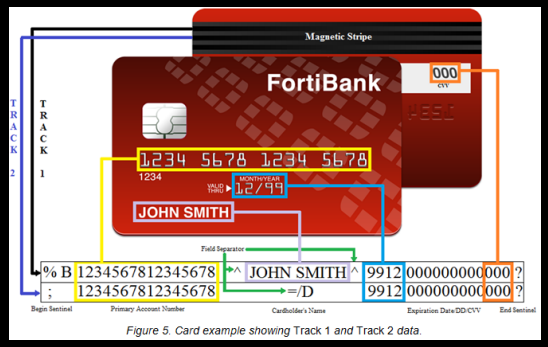


Figure 5. Card example showing Track 1 and Track 2 data.

Cybsec by Deloitte.

CASE 1: Theft of batch with credit card data

Research methodology:

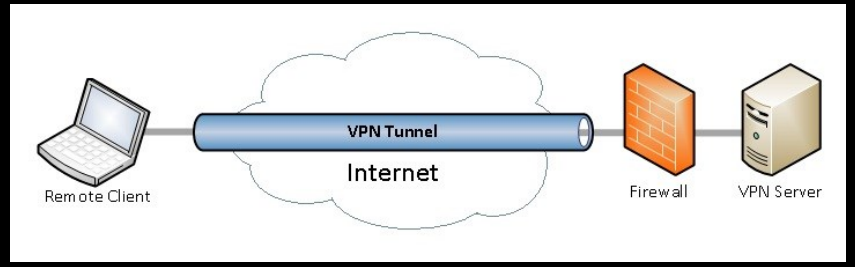
4. Data input and ticket pickup were researched and they came from different sources: in-person, online shopping, collection of tickets at the ticket office, at shows, etc..
5. Internal users who accessed the systems and system administrators were investigated to determine if they were involved.
6. Both internal systems (Reserves and Payments) were investigated and it was detected that cardholder data was still stored in plain.

Cybsec by Deloitte.

CASE 1: Theft of batch with credit card data

Research methodology:

7. The necessary corrections to erase cardholder data were made immediately and the applications were fixed so that they would not store any more data.
8. The Company's remote access systems were assessed (via vpn) and it was determined that access logs were being stored for only 30 days.
9. From the log analysis via vpn, the remote access of the provider supporting the payment system from European IPs was found.



Cybsec by Deloitte.

CASE 1: Theft of batch with credit card data

Research methodology:

10. Immediately after, we contacted the provider, who denied being the one accessing (the remote access only used user/pass).
11. Further on, by investigating the provider, it was determined that they had suffered a phishing attack through which they had been robbed of their clients' access passwords.
12. Remote accesses were blocked. Every password to access the remote systems and internal systems was changed.
13. Then, remote access was implemented using two-factor (CD).
14. We tracked the IP addresses involved and they were from Poland and Estonia.

Cybsec by Deloitte.

CASE 1: Theft of batch with credit card data

Results achieved:

In two weeks, the modus operandi of the attack was determined. From the dates of access and the logs detected we found the compromise window and over 72,000 credit cards were blocked as a preventive measure. The fraud amounted to US$ 115,000, which was covered by the insurances of the issuing Banks.

We were able to detect how the data was robbed and measures to increase the Company's security level were taken.

The criminal gang involved was from Eastern Europe. The authorities from Poland and Estonia were informed (the investigation did not succeed).

Cybsec by Deloitte.

CASE 2: Confidential information exposure

Incident description:

During a selling transaction of a Company, there was a leakage of confidential information on the process and this information was sent to employees, partners, providers, regulatory entities, etc., causing the cancellation of the transaction.

Anonymous emails with sensitive information were sent form a free electronic email account.

We began to research how the information was leaked and who was responsible for the leakage.

CASE 2: Confidential information exposure

Research methodology:

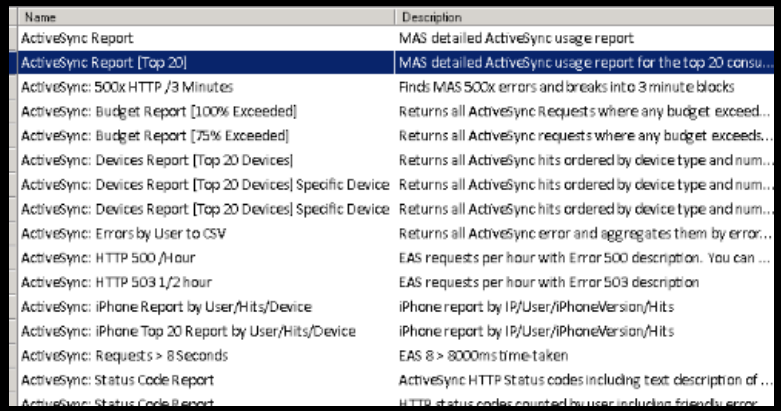
1. The emails received were analysed. It was detected that, at a technical level, detecting the source IP address was not possible. The emails and attached files were evaluated.

2. Based on this information, it was determined that several files had been created by user Jorge Rodriguez (Financial Manager) by analysing their metadata. The possible dates of information leakage were set.

3. It was determined that the user had the files in his notebook, in the email server and in his mobile device.

Cybsec by Deloitte.

CASE 2: Confidential information exposure



Name	Description
ActiveSync Report	MAS detailed ActiveSync usage report
ActiveSync Report [Top 20]	MAS detailed ActiveSync usage report for the top 20 consu...
ActiveSync: 500x HTTP /3 Minutes	Finds MAS 500x errors and breaks into 3 minute blocks
ActiveSync: Budget Report [100% Exceeded]	Returns all ActiveSync Requests where any budget exceed...
ActiveSync: Budget Report [75% Exceeded]	Returns all ActiveSync requests where any budget exceeds...
ActiveSync: Devices Report [Top 20 Devices]	Returns all ActiveSync hits ordered by device type and num...
ActiveSync: Devices Report [Top 20 Devices] Specific Device	Returns all ActiveSync hits ordered by device type and num...
ActiveSync: Devices Report [Top 20 Devices] Specific Device	Returns all ActiveSync hits ordered by device type and num...
ActiveSync: Errors by User to CSV	Returns all ActiveSync error and aggregates them by error...
ActiveSync: HTTP 500 /Hour	EAS requests per hour with Error 500 description. You can ...
ActiveSync: HTTP 503 1/2 hour	EAS requests per hour with Error 503 description
ActiveSync: iPhone Report by User/Hits/Device	iPhone report by IP/User/iPhoneVersion/Hits
ActiveSync: iPhone Top 20 Report by User/Hits/Device	iPhone report by IP/User/iPhoneVersion/Hits
ActiveSync: Requests > 8 Seconds	EAS 8 > 8000ms time taken
ActiveSync: Status Code Report	ActiveSync HTTP Status codes including text description of ...
ActiveSync: Status Code Report	HTTP status codes counted by user including friendly error...

Research methodology:

4. The email server (the web access) was analysed and no active logs were detected.

5. ActiveSync logs were assessed and analysed and it was determined that the only mobile device that connected to synchronize messages with the user jrodriguez was the correct one.

6. The notebook of Jorge Rodriguez was analysed and within the operating system logs (Security.evtx, System.evtx, Application.evtx), we detected there had been connections on dates prior to the incident.

7. The connections were made with the user “soporte” used by the IT area.

Cybsec by Deloitte.

CASE 2: Confidential information exposure

Research methodology:

8. In one of the logs, we detected the internal IP address of the computer that used the user "soporte".

9. It was determined that the computer belonged to a member of the IT support team. A forensic assessment of the computer was carried out and it was determined that, within the files deleted, files belonging to the user Jorge Rodriguez were found and that they were part of the confidential data.

10. In this computer, we also detected a user of the Dropbox system was configured. From this device, we could connect to the Dropbox system and detected several files of Jorge Rodriguez.

Cybsec by Deloitte.

CASE 2: Confidential information exposure

Results obtained :

How the data leakage process occurred could be determined.

The Company severed ties with the affected person.

Cybsec by Deloitte.

CASE 3: Deception to a company (theft of money)

Incident description:

A Company was defrauded by a group of criminals that targeted senior managers, being able to make such Company transfer money overseas (China). The first transfer was placed. The object was a secret acquisition.

The incident was accidentally detected in the middle of the second transaction, which allowed to cancel it just in time.

The modus operandi was investigated, in an attempt to track the criminals.

Cybsec by Deloitte.

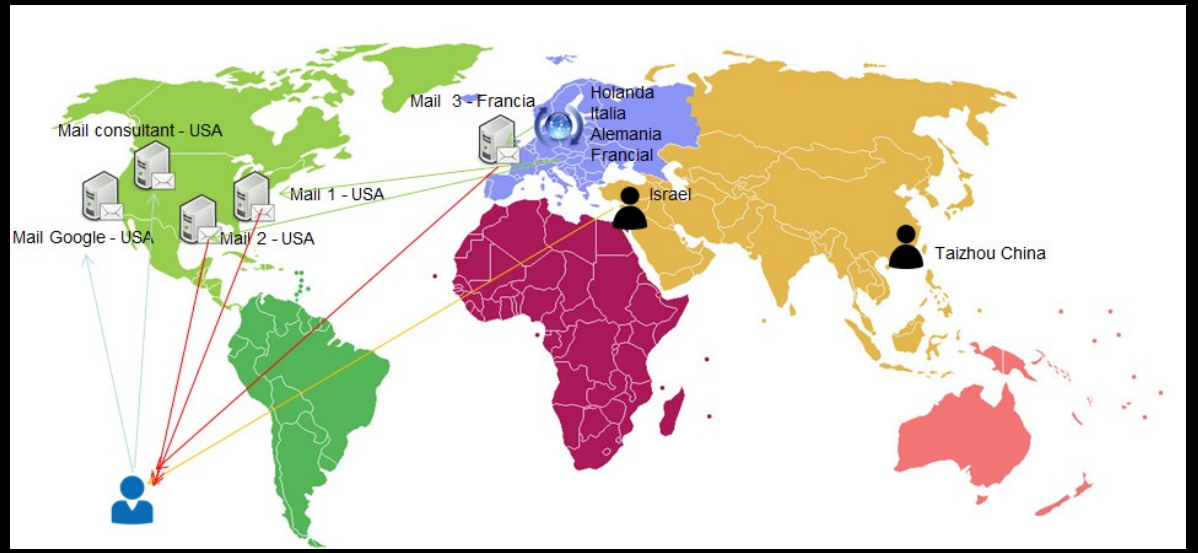
CASE 3: Deception to a company (theft of money)

Research methodology:

1. Fake email headers were evaluated (they came form valid accounts from the same domain, but the had a reply to a Gmail account).

2. The intruders had also placed telephone calls from a cell phone in Israel (which was a redirected IP number).

3. The header analysis showed that the group had used PHPmailers and Proxy to try to hide the real source IP addresses, although we detected two domains that had been used.



Cybsec by Deloitte.

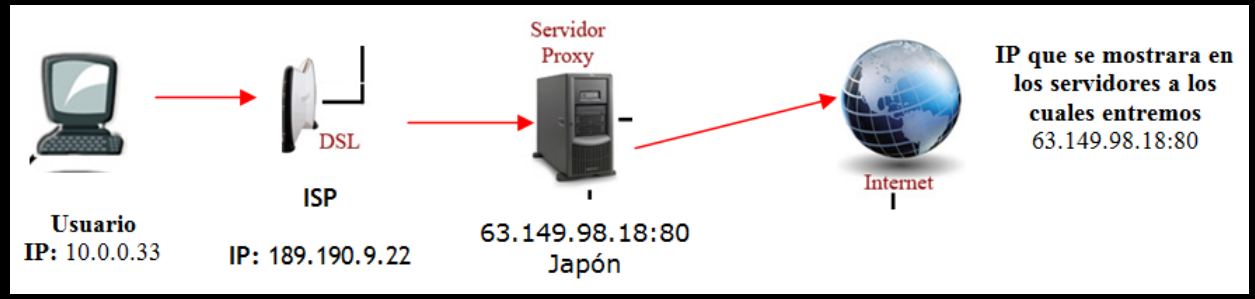
CASE 3: Deception to a company (theft of money)

Research methodology:

4. The workstations of the people that had received the fake emails with the authorizations to make the transfers were assessed in the search of malware or Trojans. Nothing suspicious was detected.

5. OWA access logs (webmail access) were analysed, and unauthorized accesses to the email accounts involved were found from the previously analysed IP addresses .

6. The detected IP addresses were analysed, and it was found that they were mainly anonymous proxy devices.



CASE 3: Deception to a company (theft of money)

Research methodology:

7. The Bank of Taizhou was contacted in order to gather further information on the funds of the first transfer, and they sent information describing that a few hours after the first transfer was placed, the money had been transferred to other 4 accounts and had been withdrawn in cash a few hours later from other branches of the Bank of Taizhou in China.

8. The domains used and the modus operandi were investigated, and was found that this is the way in which two cybercrime gangs originated in Asia operate.

Cybsec by Deloitte.

CASE 3: Deception to a company (theft of money)

Results obtained:

It was determined that the Company had been the target of a sophisticated attack that included theft of passwords, unauthorized accesses to emails, study of personal profiles and of the Organization's operating procedures.

With the first transfer, the Company lost U$S 370,000. The second one, which could be stopped, amounted to U$S 1,640,000 and the third one they were preparing amounted to U$S 13,000,000.

A formal complaint was filed in Argentina.

Cybsec by Deloitte.

Agenda

1 – Security Incidents

2 – CIR Strategy

3 – Incident Experiences

4 - Conclusions

Cybsec by Deloitte.

Conclusions

You need to get ready proactively.

Define if the investigation will be used for legal purposes.

DACM (Define – Activate – Control – Monitor) LOGS.

Define Security Incident Management Policies and Procedures.

Train yourselves and assemble the internal team (together with other areas).

Thank you

Cybsec by Deloitte.

Julio Ardita – Cybsec by Deloitte - jardita@deloitte.com