

The Price of Negligence: A Case Study on Mitigating Risk

Part 1: Incident Analysis and Response

Section A: Success of the Attack

Azumer Water, an organization of 1,073 volunteers and 10 staff members, assists urban communities with getting an adequate supply of clean water during environmental crises. They believe a water supply is vital to community repair and rely heavily on their volunteer staff to deliver bottled water within 24 hours of a disaster.

Elecktores, a hactivist group, recently began its public castigation of Azumer, criticizing them for their lack of attention to communities outside of the urban areas. They are on a mission to dissuade volunteers from being a part of the NGO and have already successfully attacked the organizations relief efforts by cancelling orders for bottled water.

Azumer Water should have been on their toes the moment they realized they were being targeted by a hactivist group; making sure they were secure and prepared to mitigate any attacks from them. Due to negligence of a very important aspect of the organization, information security, Elecktores was able to succeed in another attack; and Azumer Water paid the price.

Elecktores' strategy was to intrude Azumer through social engineering; specifically through spear phishing. They crafted an email tailored to the volunteer coordinator John Smith. The email appeared offering a deal on water pallets for a limited amount of time. This offer appeared to be from a reputable company and even created a sense of urgency, with the call to action "buy today", making it more likely to be clicked. John wasn't paying attention, and with a single click he managed to install malware. There was no Intrusion Prevention System nor was there a Intrusion Detection System put in place by their contracted IT company Pruhart Tech.

The Price of Negligence: A Case Study on Mitigating Risk

This allowed the malware to be installed unnoticed and to cause its intended damage. This could have also been the reason the attacker was able to previously cancel a water bottle shipment from a warehouse. The malware was not only able to find the databases on the local machine, but give Elecktores full access to the PII of the volunteers. This is likely due to the lack of an enforced password policy. Passwords were not being updated periodically nor were they up to a secure standard. This gave Elecktores an even higher chance of gaining access to the database. Another thing that can be pointed out is that the database was being run on an open source platform, meaning Elecktores had access to any published vulnerabilities and used it to gain access to the database.

Once Elecktores gained access to the PII in the volunteer database they were able to send out an email to all of the volunteers. They were victimized with the same technique used on John. They were presented with an email that appeared to come directly from Azumer Waters, with a sense of urgency, asking them to donate money by clicking on a link in the email. Many responded to the unfamiliar request by sending John emails, but there were a number of volunteers that fell victim to the attack leaving their payment info compromised. This was also a sign that the volunteers were not trained in any aspect of security awareness. If they were, they would have recognized the red flag that malicious links typically have a misspelled domain name or extra subdomains.

At the very least if Azumer Water had Multifactor Authentication or an enforced password policy for its databases and Intrusion Detection System this attack could have been prevented. Passwords up to secure standards would have made it that much harder for Elecktores to carry out the attack. The Multifactor Authentication would have required a second entry of a

The Price of Negligence: A Case Study on Mitigating Risk

password or a key before access was given and the IDS would have detected the malware, Unfortunately this was not the case and Azumer paid the price of being unprepared.

Section B: CIA and PII Compromise

The CIA is an aspect of information security that aims to describe the way in which information can be protected, under this model information should be protected from unauthorized access, unauthorized changes, and remain available for usage by authorized individuals. In this study all 3 aspects were compromised leaving the PII of the volunteers compromised via access to the databases.

Confidentiality was compromised when the volunteers' PII from John's computer landed in the possession of the attacker, they were not supposed to have access to this information. According to NIST 800-122 all personnel must participate in the appropriate training necessary before accessing systems that include PII. Some training on Social Engineering could have prevented this attack from happening, further training on the importance of implementing secure passwords could have prevented access to the database even if the malware was downloaded.

The Integrity of the company was compromised when the attacker presented the email as if it were Azumer Water asking for a donation from the volunteers. Availability was compromised when John no longer had access to the PII of the volunteers in the database, it was not available for him to use. NIST SP 1800-11 states there should be encrypted backups in place so that the system can be restored, in order to recover from instances of data manipulation and deletion. Azumer Water did not have any such system in place and is out of compliance with this standard.

The Price of Negligence: A Case Study on Mitigating Risk

PII was compromised when John clicked on the link, unknowingly installing the malware that would gain access to the volunteer database. The attacker by way of the malware was able to get access to sensitive info on John's computer, and through the volunteer database, the volunteers' PII. The malware gave access to their contact information, partial social security number. This proved non compliance with standard NIST 800-53, as they did not have the proper encryptions in place to protect the PII in the database, nor were they enforcing the policy on secure passwords.

Section C: Federal Regulations

Azuma Water is an NGO affiliated with FEMA and thus must be compliant with standards of the Privacy Act of 1974 and the Federal Information Security Management Act.

The Privacy Act states that individuals have the right to be protected from unauthorized access to their personal information and to be protected from unauthorized usage of their personal information. Under the act Azumer is supposed to have proper protection in place to protect the PII of the volunteers. That protection is further defined in the Federal Information Security Management Act, as it states what types of programs and procedures can be put into place to implement protection. As an example of compliance, the database could have been encrypted, a MFA in place, and an intrusion detection system so the InfoSec team can act quickly to stop any attempts to access that information. This would all be to prevent the PII from being in the hands of those that should not have it. The success of the attack shows Azumer Water, in fact, did not have the proper protocols in place to protect the PII of the volunteers, rendering them out

The Price of Negligence: A Case Study on Mitigating Risk

of compliance with the Privacy Act of 1974 and the Federal Information Security Management Act.

Section D: Mitigation Steps

According to the NIST standard of incident response, the first step in the case study would be to detect the threat/attack, then contain the threat, eradicate the threat, and begin the recovery process. Though the case study lacks a proper plan in place that is up to NIST standards these steps can still be performed to some degree. The malware has already been downloaded and the email has already been sent to the volunteers. We have already detected the threat. In this case, containing the threat means making sure no one else clicks the link sent in the email to the volunteers, and that if the link was clicked, that no one else enters their credit card information or personally identifiable information. Assuming there is a tangible emergency contact list at the main office of the NGO, everyone would need to be contacted. To begin eradication, and as a first step to heighten security posture, antivirus software would have to be installed. This would be run on all devices that clicked the link to make sure any malware that was installed is completely removed. Lastly, because there is no backup of the data, the recovery process would have to involve the restructuring/rebuilding and encryption of the database.

The Price of Negligence: A Case Study on Mitigating Risk

Section E: Incident Response

If the proper infrastructure was put into place with Pruhart the first time around, the Incident Response would have gone as such.

Identify: The assets risks and vulnerabilities would have been identified and protocols put in place that align with business needs, have the support of the upper level management, and are in line with the budget in the finance department; a plan would be in place to mitigate attacks.

Protect: Safeguards are implemented to help protect the infrastructure put together in the Identify step. This includes supporting aspects like Access Control or Awareness and Training.

Detect: Observational Technical Tools such as Intrusion Prevention Systems and Intrusion Detection Systems would be used to monitor the network, server, and workstation activities, to look for unusual activity in real time; they would be blocked or an alert sent when a condition matches a set parameter. I would also implement availability monitoring to make sure the information systems are available and running properly.

Respond: The immediate response is to prevent further harm to the organization. This is where containment and eradication come in. The threat would be contained so that it could not spread damage elsewhere or further damage the information systems, it would then be eradicated.

Eradication can be a very critical part of the response as you want to make sure that all parts of the threat are removed in every way to ensure the attacker isn't maintaining any sort of anchorage in the system.

Recover: After the containment and eradication of the threat, the recovery process would begin; bringing the information system back to its normal state where it is completely operational.

The Price of Negligence: A Case Study on Mitigating Risk

Part 2: Risk Assessment and Management

Section F: Federal Regulations Compliance

Azumer was not at all in compliance with The Privacy Act 1974 nor was it in compliance with the Federal Information Security Act. This was due to a lack of processes and technical solutions in place to prevent the acquisition of PII from the database. There were no safeguards to prevent one from getting to the database and no safeguards to protect the PII in the database. In order to bring Azumer to compliance with the Federal Information Security Act, an information security plan would need to be developed, security awareness training implemented and a response to incidents that ensured business continuity, such as system back ups. Furthermore Azumer's compliance with The Privacy Act of 1974 would depend not only on the implementation of compliance requirements for FISMA, but also, not allowing the disclosure of PII to unauthorized individuals. Each person that accesses PII must be trained.

Section G: Technical Solutions

There are quite a few solutions that can be implemented and become a significant part of the overall infrastructure of the NGO.

Configuration of Firewall: If the firewall is not being used and/or is not configured properly it is not doing its job. Configuring the firewall would allow it to filter, monitor, and control the network traffic to protect the organization from external threats.

Encrypting All Data in the Database: The database is not encrypted, which is why Elecktores was able to gain access to the PII of the database. Encryption would provide a layer of protection around the data making it that much harder to access by an unauthorized individual.

The Price of Negligence: A Case Study on Mitigating Risk

Installation of Antivirus Software: The installation on any and all devices used in the office would allow detection and removal of malware, ransomware, and other viruses.

VPN: Implementing a Virtual Private Network would allow for secure access to work from a home office and lessen the risk of any sensitive information being compromised through an insecure home network.

Upgrading WEP to WPA: WEP is deprecated and can be easily bypassed with the simplest of knowledge or tools. A better option by today's standards would be WPA. WPA is a newer standard that is much more secure.

Implementation of Backups: Backups are crucial to this NGO as they rely heavily on the information in the database to place orders, organize and dispatch their volunteers, and to overall keep track of the organization. In the event that data is manipulated or deleted. The database can be restored from a backup allowing operations to continue as they were.

Intrusion Prevention Systems and Intrusion Detection Systems: IPS and IDS would be used to monitor the network, server, and workstation activities, to look for unusual activity in real time; certain instances would be blocked or an alert sent when a condition matches a set parameter.

Section H: Organizational Structure

Taking into account the size of the organization, I would change the organization to include more defined roles and just enough roles to get the job done. **General users** fulfill any responsibilities and expectations set forth by policies and procedures in regards to security awareness. General users are anyone apart of the NGO that does not have a more specific role. Though they may not

The Price of Negligence: A Case Study on Mitigating Risk

have a specific role they are still a part of the collective NGO and equally responsible for playing their part in information assurance. There would also be **IT staff** and **Upper Management**. IT Staff would be responsible for prevention, detection, and making sure policies met federal standards and are implemented. The IT Staff would include one or two IT professionals and the Pruhart Company. This team would make sure the information assurance infrastructure is solid and serves its purpose according to the needs of the organization, all while making sure the right assets are protected to the most sensible degree. The final team would be Upper Management. This team would work directly with both the IT team and the board members of the NGO to make sure that everyone is in support of policies and procedures and that they are being implemented in the best way possible according to the needs of the organization in terms of its finances and mission. This would also be the team that helps to enforce policy on and educate the general users.

The Price of Negligence: A Case Study on Mitigating Risk

Section I: Risk Management

Manipulation/Loss of Database:

This *risk* would involve the manipulation of or deletion of the volunteer database. Considering the database is not encrypted, the *likelihood* of this becoming an issue through someone's unauthorized access is highly likely, the *impact* would be high and *quite severe* as the NGO operates because of the service of the volunteers. Not being able to contact them, means the NGO ceases to operate.

Successful Phishing Attack:

The *risk* would involve a successful phishing attack where malware or ransomware is installed. The *likelihood* of this happening is high due to the fact that all volunteers and employees have not completed security awareness training. The severity of this instance would be high as there are currently no safeguards in place to prevent or mitigate this attack. The impact would be high as well; if malware causes a breach in data, or malware it can be misused, manipulated, or deleted completely.

PII Breach:

The *risk* would involve PII being exposed to unauthorized personnel. The *likelihood* of this happening is quite high due to the fact that there are no protections in place for this data. There are no secure passwords or keys protecting it. The *severity* and *impact* would be high because it would render the NGO out of compliance with several federal regulations and could even leave individuals vulnerable to identity theft.

The Price of Negligence: A Case Study on Mitigating Risk

Management of Risk:

The Management of these risks would involve the implementation of secure passwords, encryption of databases, security awareness training, and antivirus software.

The Price of Negligence: A Case Study on Mitigating Risk

Sources

Computer Security Division, I. T. L. (2016, November 30). *Prepare Step - NIST Risk*

Management Framework | CSRC | CSRC. CSRC | NIST.

<https://csrc.nist.gov/Projects/risk-management/about-rmf/prepare-step>

Draft NIST Special Publication 800-53 Security and Privacy Controls for Information

Systems and Organizations JOINT TASK FORCE. (n.d.).

<https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>

FISMA & NIST Standards. (n.d.). CompliancePoint.

<https://www.compliancepoint.com/regulations/nist/>

Framework for Improving Critical Infrastructure Cybersecurity. (2014).

<https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

Imperva (2020, June 17). *What is phishing: Attack Techniques & Scam examples: Imperva*. Learning

Center. Retrieved October 25, 2021, from

<https://www.imperva.com/learn/application-security/phishing-attack-scam/>.

McBride, T., Ekstrom, M., Lusty, L., Sexton, J., & Townsend, A. (2020). *Data Integrity:*

Recovering from Ransomware and Other Destructive Events.

The Price of Negligence: A Case Study on Mitigating Risk

<https://doi.org/10.6028/nist.sp.1800-11>

Mccallister, E., Grance, T., & Scarfone, K. (2010). *Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Recommendations of the National Institute of Standards and Technology*.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>

NIST 800-53: A Guide to Compliance. (n.d.). <https://Blog.netwrix.com/>.

<https://blog.netwrix.com/2021/03/03/nist-800-53/>

Scarfone, K., Grance, T., & Masone, K. (2008). *Archived NIST Technical Series Publication Archived Publication Series/Number: NIST Special Publication 800-61 Title: Computer Security Incident Handling Guide Superseding Publication(s) Title: Computer Security Incident Handling Guide Additional Information (if applicable) Withdrawal announcement (link): N/A*. <https://doi.org/10.6028/NIST.SP.800-61r1>

Security and Privacy Controls for Information Systems and Organizations. (2020).

<https://doi.org/10.6028/nist.sp.800-53r5-draft>

The Privacy Act of 1974. (n.d.). Osc.gov. <https://osc.gov/Pages/Privacy-Act.aspx>

What are FISMA Compliance Requirements? | SolarWinds. (2016). Solarwinds.com.

<https://www.solarwinds.com/federal-government/solution/fisma-compliance-requirements>

ents