Part 3a Assessment Task

*i) Discuss what steps you could take to immediately alleviate the impacts of the attack on the business.*

The primary objective is business continuity, to maintain the business critical processes which are necessary for customers to do business. It can be observed in table 1, a combination of the Firewall Log for Firewall 1 (FW1) and IP-Lookup information, that the malicious traffic spawns from multiple Internet Protocol (IP) addresses but all originate from a common port number. I would ask the network team to re-configure the edge routers to drop all incoming packets from any IP addresses originating from source port 9999 or black hole the malicious traffic and send it to the null0 interface. Stopping the malicious traffic could also be achieved by modifying the routers Access control list (ACL), but this is known to increase the load on the router (Davis, 2008). Another possibility is calling the Akamai DDoS Attack Hotline (+61-290089630) for emergency DDoS protection if it could be guaranteed that the Board would release funds to allow it, with a typical response time of around one hour (Akamai, 2017).

Table 1. indicates destination ports 23 and 80 of the malicious traffic. Port 23, used by telnet and port 80, used by http. Harden the edge router, port 23 should be unnecessary on mail server so close if not required and thus reduce the attack surface or if necessary change protocol to Secure Shell (SSH) which affords some protection via encryption. Could use default port 22 or a safer option choose an alternate outside the most common ports.

Call Internet Service Providers (ISPs) and ask for their help to stop the inbound malicious traffic if they can’t do it immediately then look at options for cloud based mitigation while shopping around for ISP’s make sure to notify them of the relevant.

*Discuss the further steps you would take to stop the incident and get the network back to a stable operating state.*

These secondary objectives are more closely tied to Disaster Recovery (DR), to get all the other services back up and back to business as usual. Also make any other necessary improvements in order to reduce the risk of a similar incident in the future. If the current ISP/s can’t provide D/DoS protection, its time to shop for different vendors that have it included and up rate incoming bandwidth from ISP’s while we are at it.

Cloud mitigation Akamai D/DoS prevention and Fast DNS, auto rate limiting to drop specific IP’s if traffic gets above a predetermined threshold. Whitelisting known-good Domain Name System DNS resolvers. (Akamai, 2017). There would be some obvious time delay to get Akamai up and running as a solution with how slow boards move to hand out money, hence being a secondary concern and not an immediate solution. I would choose Akamai as a solution over other vendors, because it’s hard to pass the vendor who stopped the world’s largest DDoS (Feb 2018), 1.35Tbps attack within 8 seconds (Akamai, 2019).

Do a full audit of the companies security administrative controls, policies and infrastructure to evaluate the current position when compared to Payment Card Industry Data Security Standard (PCI DSS) requirements. (PCI Security Standards Council, 2018). This activity would need to be outsourced to consultants as we are unlikely to have the technical expertise to ensure we are compliant and pass accreditation.

The company needs to consider upgrading its technical infrastructure and evaluate a variety of avenues through which this could be achieved.

* Modifying the network architecture, increasing the number of vlans if possible thereby changing the number of collision domains and reducing network load.
* Upgrading the backbone of the network architecture, increasing the capabilities of the edge router and firewalls, which would reduce the network load.
* Engage consultants to make other suggestions on how to add greater redundancy, more efficient load balancing and reduce the number of single points of failure.
* Retrofitting the network with a higher rated cable type, though this would likely prove costly depending on the pre-existing type.

*ii) Discuss a communication strategy that would ensure communication to everyone in the organisation about the nature of the problem how it will be fixed and the time it would take to fix it.*

In the age of social media it is important to have a good communication strategy to notify all relevant stakeholders and keep them up to speed. There needs to be a concise statement of the nature of the incident, an estimated time it will be resolved and for technical staff, a description of how it will be re mediated. In the present case, the company is currently under D/DoS attack from a malicious outsider affecting all company internet related services and it should be resolved within two hours. This is necessary to avoid brand damage from unhappy stakeholders, disseminating rumours and lost time and resources due to double-handling of tasks internally. The communication strategy needs to be broken down into two key areas comprising:

* Internal: company staff, technical (newly formed interdisciplinary Incident Response Team, security, network, mid-range, application development, contact centre, telephony, facilities management), legal, marketing, public relations, board members.
* External: Customers, partner companies, shareholders, media, Internet service providers, managed service providers (if any), related compliance testing providers, consultants, reporting authorities, law enforcement and associated regulatory bodies.

Firstly, there is no indication that there is any preexisting pager infrastructure, so we can rule that out as a communication medium. At the outset of a subsequent incident, short message service (sms) should be used for immediate alerts as the telephony system is not impacted and everyone has a mobile device. Phone calls can be made if further clarification is required and follow-up with more complete reports via email as the delay will not have significant impact.

The Incident response team should meet in an Incident Response Room, temporary for now but there is a need to discuss provisioning a dedicated space at a later date. This should begin at the declaration of an incident and then continue daily until the situation has been resolved. There is a need to inform the technical teams, keep them updated and have them reciprocate.

Most external communication will be handled by the marketing or public-relations team. It will be necessary for technical teams and the legal department to aid them in constructing a non-technical statement including a brief description of the nature of the incident and an estimate of when it will be resolved. This is to be delivered to affected customers and media via sms and electronic media (email, social media). Post incident, we will need to post a notification in a prominent position on the company website explaining the outage once the D/DoS attack has been mitigated. There may need to be a separate more technical explanation released to external business partners so they can respond accordingly.

The security team are to inform the ISP’s of a D/DoS attack in progress and request assistance in blocking the attack. The regulatory compliance, law enforcement and reporting bodies will need to be informed of the incident by the businesses legal counsel as set out in the standards.

Part 3b Assessment Task

i) *Construct an Incident Response Plan specific to the security incident mentioned in the case-study. What technical design and implementation aspects, administrative controls and documentation could be improved in order to limit, or eliminate, the impact of such an attack in the future?*

From the background provided in Case Study Part 1, it is clear the company had no documented Disaster Recovery or Business Continuity Plan, there was no formal Incident Response Team or Incident Response Plan and limited documentation on the current network system other than the topology prior to this incident. There is also no security base-line monitoring except for the currently available logs and the security culture of the business is poor at best. These are all part of the policies and frame-works that should already be established for the business to have gained PCI DSS compliance.

The aspects that need immediate attention are:

* Formalising the formation of an Incident Response Team
* Drawing up a Disaster Recovery Plan
* Drawing up a Business Continuity Plan
* Drawing up an Incident Response Plan
* Drawing up a change management plan
* Establish security baseline monitoring so there is something to compare anomalous traffic and logs to later
* Establish inventory control on all devices inside the network perimeter
* Organise some level of Cyber Insurance to transfer risk
* Examine strengthening our incident response frame-work with a threat intelligence
* A cyber security or user awareness training program needs to be integrated with the onboarding process for new employees.
* Set aside private, dedicated space for an incident response room, to limit premature dissemination of information regarding the incident.

Draw up our IRP using the methodology National Institute of Standards and Technology (NIST). Maintain an up to date paper copy of the incident response plan in the advent of an incident making it impossible to use a digital copy. Keep a back-up copy of the incident response plan on usb stick, to be carried by the Incident Response Team Leader. Summarise the content into an actionable flip-chart to be kept in “war room”. Print posters with emergency contact information to be displayed at key locations.

**INCIDENT RESPONSE PLAN**

**Denial of Service & Distributed Denial of Service**

**Black Stump Banking (BSB)**

# **Ownership and** **Approval**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Policy Owner and Title | Phone | Email | Date | Signature |
| Security Team Manager | 123456789 | security.m@blackstumpbanking.com.au |  |  |
| Approved By |  |  | Date | Signature |
| Executive |  |  | 16/05/2019 | Someone’s Signature |

# **Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Description | Policy # | Revision Date | Review  Date | Reviewer/  Approver Name |
| 1.0 | Initial Version |  | 16/05/2019 |  | Someone’elses Signature |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# **Compliance & Reporting**

|  |  |
| --- | --- |
| Compliance Rule | Description |
| PCI DSS | Provides organizations that accept, store or transmit credit card data with guidelines for privilege management and a framework to protect cardholder data. <https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf> |
| ACORN | Australian Cybercrime Online Reporting Network. For reporting cyber incidents and threats Australia-wide. <https://report.acorn.gov.au/> |
| NIST SP 800-53 | The National Institute of Standards and Technology (NIST) outlines steps in NIST SP 800-53 including reporting requirements,a standard set of data elements that must be included in any incident report.  <https://www.us-cert.gov/incident-notification-guidelines-2015> |

**EXECUTIVE SUMMARY**

To maintain the trust of our employees, customers, and external partners, and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a Denial of Service incident moving forward. The more we are prepared to respond to a potential incident, the faster we can eradicate any threat and reduce the impact on our business.

The goal of this incident response plan is to prepare Black Stump Bankingto quickly and effectively combat a Denial of Service style attack while maintaining business continuity. To this effect, actions outlined in the plan pay special attention to protecting the critical functionality of systems such as our web based customer services, partner application server, corporate servers and network.

Effective incident response involves every part of Black Stump Banking, including our IT technical teams, legal, technical support, marketing and public relations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be updated quarterlyto reflect our changing company-wide posture towards new technologies and new compliance requirements and a strong cyber security strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

**ROLES, RESPONSIBILITIES & CONTACT INFORMATION**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibility** | **Contact Details** |
| **Information Security** | | |
| Chief Information Officer (CIO) | Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritise incident response plan.  Authorises when and how incident details are reported.  Main point of contact for executive team and Board of Directors. | Name:  Phone:  Email: |
| Incident Response Team Leader and Team Members | Central team that authorises and coordinates incident response across multiple teams and functions through all stages of a cyber incident.  Maintains incident response plan, documentation, and catalogue of incidents.  Responsible for identifying, confirming and evaluating extent of incidents.  Conducts random security checks to ensure readiness to respond to a cyber attack. | * CIO * Security Manager * Network Manager * Mid-Range Manager * Legal Counsel * Public Relations Liason |
| Security Team Manager | Responsible for privilege management, enterprise password protection and role-based access control.  Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are.  Proactively checks for indicators of compromise.  Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks.  Takes action to prevent the spread of a breach by updating privileges. | Name: Robert Shannon  Phone:  Email: |
| Network Team Manager |  | Name:  Phone:  Email: |
| Mid-Range Team Manager (IT Support) | Manages access to systems and applications for internal staff and partners.  Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyber attack. | Name: Felix Canterford  Phone:  Email:  Team Members:  Rolf & Peter |
| Application Team Manager | Responsible for any bespoke or in-house written applications. | Name: Peter Thompson  Phone:  Email: |
| Contact Centre Team Leader | Responsible for call centres | Name:  Phone:  Email: |
| Telephony Team Leader | Responsible for the telephony systems | Name:  Phone:  Email: |
| Facilities Managment Team Leader | Responsible for the management of physical facilities | Name:  Phone:  Email: |
| Technical Partners (Internet Service Provider, Managed Service Providers, Hosting, Testing Partners, etc.) | Manages security controls to limit progression of a cyber attack across third-party systems and organisations. | Name:  Phone:  Email: |
| Consultants | Any Consultants who’s services are retained for expertise outside the companies current technical capabilities including Digital Forensics | Name:  Phone:  Email: |
| **Compliance & Reporting** | | |
| Legal Counsel | Confirms requirements for informing employees, customers, and the public about cyber incidents.  Responsible for checking in with local law enforcement.  Ensures IT team has legal authority for privilege account monitoring.  Communicates with regulatory bodies, following mandated reporting requirements. | Name:  Phone:  Email: |
| ACORN (Australian Cybercrime Online Reporting Network) | Receives information about an incident according to timeline and format mandated by regulatory requirements. | Name:  Phone:  Email:  <https://report.acorn.gov.au/> |
| PCI DSS (Payment Card Industry Data Security Standard) | Receives information about an incident according to timeline and format mandated by regulatory requirements. | Name:  Phone:  Email:  [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf) |
| **Communications** | | |
| Marketing & Public Relations Lead | Communicates externally with customers, partners and the media.  Coordinates all communications and request for interviews with internal subject matter experts and security team.  Maintains draft crisis communications plans and statements which can be customised and distributed quickly in case of a breach. | Name:  Phone:  Email: |
| Web & Social Media Lead | Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users.  Sets up monitoring across social media channels to ensure we receive any feedback or questions sent by customers through social media. | Name:  Phone:  Email: |
| External Partner Companies |  | Name:  Phone:  Email: |

**RISK ASSESSMENT**

Availability – Incidents that impact availability or proper functioning of services, such as Distributed Denial of Service (DDoS). The more critical the services to the business, the higher the potential impact.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CYBER INCIDENT** | **CIA CATEGORY** | **PRIVILEGED ACCOUNT BREACH** | **BUSINESS IMPACT** | **RISK LEVEL** |
| Denial of Service, disrupting business services or resources by flooding with incoming traffic in an attempt to overload systems. | Availability | No | Medium | Low |
| Distributed Denial of Service, disrupting business services or resources. The incoming traffic flooding the service or resource originates from many different sources. | Availability | No | Medium | Low |

**ACTION PLAN**

In order to demonstrate and improve the effectiveness of Black Stump Banking’s incident response team and security tools, Black Stump Banking requires meticulous records of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, vulnerability scans, audits, network traffic, and disk images.

Below is the reporting checklist to use when documenting actions taken to combat a declared incident. At Black Stump Banking, it is our goal to meet compliance requirements and prioritise business continuity in order to minimise impact and cost.

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase of Cyber Incident** | **Action** | **Team Member/System** | **Day/Time**  **Action Taken** |
| **Incident Discovery and Confirmation** | Describe how the team first learned of the attack (security researcher, partner, customer, auditor, internal security alert, etc.) |  |  |
| Analyze audit logs to identify unusual or suspicious account behaviour that indicates a likely attack and confirm attack has occurred. |  |  |
| Describe potential attacker, including known or expected capabilities, behaviours, and motivations. |  |  |
| Identify access point and source of attack (endpoint, application, Ip addresses, etc.) and responsible party. |  |  |
| Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites. |  |  |
| Evaluate extent of damage upon discovery and risk to systems. |  |  |
| Inform employees regarding discovery. |  |  |
| Share information externally about the attack. You may choose to hold communications during this phase until you have contained the incident in order to increase your chances of catching the attacker. if so, make sure that aligns with your compliance requirements. |  |  |
| **Containment and Continuity** | Protect evidence. Back up any affected systems as soon as possible, prior to performing any actions that could affect forensic data integrity on the original media. |  |  |
| Increase the sensitivity of application security controls (whitelisting blacklisting, and greylisting) to prevent malicious malware from being distributed by the attacker. |  |  |
| Remove systems from production or take systems offline if not needed for business continuity. |  |  |
| Inform employees regarding breach containment. |  |  |
| Share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |
| **Eradication** | Close firewall ports and network connections. |  |  |
| Test devices and applications to be sure that the attack has been mitigated. |  |  |
| Compare security base-lines before and after the incident to ensure systems functioning normally. |  |  |
| Inform employees regarding eradication. |  |  |
| Share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |
| **Recovery** | Apply security patches if required. |  |  |
| Close network access and reset passwords. |  |  |
| Conduct vulnerability analysis. |  |  |
| Restore any systems or services that were taken offline. |  |  |
| Inform employees regarding recovery. |  |  |
| Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |
| **Lessons Learned** | Review forensic evidence collected. |  |  |
| Assess incident cost to business. |  |  |
| Report to executive team and auditors if necessary. |  |  |
| Implement additional training for everyone involved in incident response and all employees. |  |  |
| Update incident response plan. |  |  |
| Inform employees regarding lessons learned, additional training, etc. Include this in future security awareness training. |  |  |
|  | Share information externally (website updates, emails, social media posts, tech support bulletins, etc.) |  |  |

**POST INCIDENT REVIEW**

*ii) Discuss possible problems you may face in improving the overall security posture of the bank and how you would deal appropriately with them.*

There is a vast array of possible obstacles when considering an overhaul of the overall security posture of the company. The main challenge categories being: technical, administrative, budgetary and cultural, with perhaps the biggest hurdle being cultural change. There is always going to be resistance to change, people become entrenched in the way they approach their tasks and negative reactions towards tightening of security protocols result if they feel it is too restrictive or are perceived to lower their productivity. Users don’t like overly complicated solutions, they always follow the path of least resistance and delight in obfuscating security controls if they feel they are too restrictive. Friction is often the enemy of productivity.

As a company we need to highlight the importance of cyber security to business success. We need to show employees that it is a key concern by making awareness training part of the on-boarding process and roll out yearly security awareness training for existing staff. To aid increasing awareness of the companies new approach, we should instituting a phishing simulation serve as monthly reminder that Black Stump Banking takes it seriously. Too long security has been seen as solely as the responsibility of the security team. The CIO the and C-suite need to recognise that it is as necessary for them to lead by example, and exhibit this new attitude towards developing a strong security culture.

All of these new frame-works, policies, procedures and plans will eat into the corporate budget. Convincing the C-suite to part with enough money to be able to implement them effectively will be a real challenge. We need to be able to rationalise these costings to Board and show them the value of mitigating risk to their bottom line. We must contrast the cost of the business implementing these new security controls with the cost of doing nothing, the average cost of a cyber security incident is increasing. The negative impacts including increased insurance cost, negatively impacting company share price. There are a range of other expenses that will need evaluating and ultimately to be budgeted for:

* upgrading infrastructure, engaging consultants in re-designing network topology.
* providing Incident response team with dedicated space for Incident Response
* SIEM or baseline monitoring,
* vulnerability scans and penetration testing.

Back up this by providing costing estimates calculated losses resulting from this most recent incident by D/DoS. Highlighting the net effect on stakeholders, the disruption to service and customers, reduced share price, increased insurance premiums.

The current level of technical expertise, the teams strengths and weaknesses will need to be assessed and technical gaps, filled by outsourcing to consultants or in the form of new hires. Another way to combat the gaps in our teams technical knowledge would be to offer to fund them to upskill and complete relevant training and certifications. Other technical challenges that will be faced when trying to improve company security include, the need to identify what assets the company has as you can not effectively protect the unknown. Currently staff may not have the technical capabilities to roll-out an educational security awareness campaign or phishing simulations without some level of assistance, so these will most likely need to be outsourced to specialist consultants. An evaluation will need to be carried out to establish what the executive team consider to be an acceptable amount of time for our business services to be knocked offline by a Denial of Service style attack. This will allow the security team to identify what level of DoS attack protection is required, always on or on demand.

The primary administrative challenge will be getting someone to sign off on a Disaster Recovery and Business Continuity Plan. “It is critical for the C-Suite to establish compliance with standards and policies as a key corporate value”(McCarthy 2012). As security of customers financial data is the foundation of the business. PCI DSS compliance has a contractual reporting obligation. To combat C-suite level push back I would direct them to an Executive Summary of the Verizon Data Breach Investigations Report (Verizon, 2019) and follow up with a quick summary of the Sony Playstation DDoS attack (Davis, 2016).

Table 1



References

Akamai. (2019). *Inside the Largest DDoS Attack in History* [Video file].Retrieved from https://akamai.com/us/en/resources/

Akamai. (2017). *Making a DDoS Protection Plan: 8 Best Practices.* Retrieved from https://akamai.com/us/en/resources/

Chaitow, J. (2019) *There’s a hole in my infrastructure? The road to PCI Compliance.* Retrieved from SANS Institute https://www.sans.org/reading-room/whitepapers/compliance/hole- infrastructure-road-pci-compliance-32834

Cheswick, W. R., Bellovin, S.M., & Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker* (2nd ed.) Addison-Wesley Professional.

Chou, E. & Groves, R. (2018). *Distributed Denial of Service (DdoS): Practical Detection and Defence*. O’Reilly Media. Retrieved from https://www.a10networks.com/sites/default/files/ A10-TPS-EB-Distributed\_Denial\_of\_Service\_DDoS\_Practical\_Detection\_and\_Defense.pdf

Davis, D. (2008). *Black hole routes: The good, the bad, and the ugly.* TechRepublic. Retrieved from https://techrepublic.com/blog/data-center/black-hole-routes-the-good-the-bad-and-the-ugly/

Davis, J. (2016). *Sony PSN downed; hacking group claims DDoS attack.* Retrieved from SCMagazine https://www.scmagazine.com/home/security-news/sony-psn-downed- hacking-group-claims-ddos-attack/

Eddy, W. (2007). *TCP SYN Flooding Attacks and Common Mitigations.* Verizon. Retrieved from https://tools.ietf.org

IP-Lookup.net (2019) *Lookup an IP address.* https://ip-lookup.net/index.php

McCarthy, N.K. (2012) *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk.* McGraw-Hill. Retrieved from Safari Books Online.

Moriarty, K.M. (2004) *Distributed Denial of Service Incident Handling: Real-Time Inter-Network Defence.* MIT Lincoln Laboratory. Retrieved from https://tools.ietf.org

Neustar Security. (2019). *Art of Darkness: Understanding the DDoS Threat.* Neustar, Inc. Retrieved from https://bankinfosecurity.com

Northcutt, S. (2003). *Computer Security Incident Handling: An Action Plan for Dealing with Intrusions, Cyber-Theft, and Other Security-Related Events.* Retrieved from SANS Institute https://www.sans.org

Pandya, G. (2019) *Preparing to Withstand a DDoS Attack.* Retrieved from SANS Institute https://www.sans.org/reading-room/whitepapers/incident/preparing-withstand-ddos-attack- 36412

Pace, C. (2018) *The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence.* Cyber-Edge Press.

PCI Security Standards Council (2018) *Payment Card Industry Data Security Standard: Requirements and Security Assessment Proceedures V 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCI\_DSS\_v3-2-1.pdf*

PCI Security Standards Council. (2019). In PCIComplianceGuide.org. Retrieved from https://www.pcicomplianceguide.org/faq/

Prowse, D. L. (2018). *CompTIA Security+ SY0-501 Cert Guide.* Pearson. Retrieved from Safari Books Online.

SANS Institute. (n.d.) “Score: Checklists & Step-by-Step Guides” retrieved from https://www.sans.org/score/checklists

Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World.* Wiley Publishing.

Thycotic.com (2019). *Customizable Cyber Security Incident Response Plan Template.* Retrieved from *https://thycotic.com/solutions/free-it-tools/free-privileged-account-incident-response- policy-template/*

Vazquez, M. (2019). *IDC MarketScape: Worldwide DDoS Prevention Solutions 2019 Vendor Assesment.* Retrieved from https://www.bankinfosecurity.com

Verizon. (2019) *2019 Data Breach Investigations Report.* Retrieved from https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf