Data Breach Incident Management Policy

Data Breach Management Guidelines

Original author's name:	Pkkirisankar Jagannath
Most recent date:	November 22, 2022
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	November 22, 2022	Pkkirisankar Jagannath	Original Draft
v1.0	November 22, 2022	Kulpreet Singh	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	November 22, 2023

POLICY STATEMENT

1. This guidance is intended to supplement the Organisation of TSCTI Data Protection and other information security policies, and has been developed in the aim of aiding the understanding of the Organisation's obligations in the event of a data security breach.

2. These guidelines apply to all members of the Organisation. All contractors and agents acting for or on behalf of the Organisation should be made aware of these guidelines and the Organisation's Data Protection Policy.

3. This policy applies to all methods of processing of personal information, on any device, whether Organisation or personally owned, which is used for Organisation purposes, whether, on a regular or an ad-hoc basis.

4. The General Data Protection Regulation and the Data Protection Bill require that personal data is processed fairly and lawfully and, in particular, not be used or processed in ways which would have unjustified adverse effects on the individuals concerned.

1. BREACH OF DATA

1.1 A personal or sensitive data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the purposes of the Organisation business.

1.2 Members of staff at the Organisation, who access, hold or process personal or sensitive data for the purposes of the Organisation business must take appropriate steps to ensure no unauthorised or unlawful processing, accidental loss, destruction of, or damage to personal data occurs.

1.3 A personal data breach can occur for a number of reasons, such as:

a) Loss or theft of data or equipment on which data is stored;
b) Inappropriate access controls allowing unauthorised use;
c) Equipment failure;
d) Human error;
e) Unforeseen circumstances such as fire or flood;
f) Hacking attach;
g) Offences where information is obtained by deceiving the holder of theinformation, the Organisation.

2. CONTAINMENT AND RECOVERY

2.1 Data security breaches should be contained and responded to immediately upon discovering the breach. An Impact Assessment should be undertaken to identify measures required to contain or limit potential damage, and recover from the incident.

2.2 All data breaches, actual and potential, must be reported to the the Data Protection Officer (dataprotection@tscti.com) via the below Data Breach Incident Reporting Form and the IT Department, where appropriate.

3. ASSESSING THE RISK

3.1 Some data security breaches may not lead to risks beyond possible inconvenience tothose who need the data to undertake their role (i.e. a laptop is irreparably damaged, but its files were backed up and can be recovered). Following immediate containment, the risks must be assessed which may be associated with the breach, Potential adverse consequences to the individuals, as well as, the Organisation itself, and the seriousness of the breach must be considered, further to immediate containment.

3.2 The following must be considered upon discovering a data breach:

a) The type of data involved;

b) Whether the data is sensitive

c) If data has been lost or stolen, whether encryption protections are in place;

d) What has happened to the data, such as the possibility that it may be used tocause harm to the individual(s);

e) The level of detail that would be exposed and how this could affect theindividual

4. NOTIFICATION OF DATA BREACHES

4.1 Upon the completion of an Impact Assessment by the Program manager or the Data Protection Officer, breaches capable of adversely affecting the individuals should be communicated to those individuals for the purposes of ensuring thatspecific and clear advice is provided on the steps to be taken to mitigate the risks and if any support could be provided.

4.2 It must be evaluated whether the Information Commissioner's Office, other regulatory bodies, and/or other third parties such as the Police or bank/building societies should be notified of the data breach.

4.3 Serious breaches may require for a ‘media message’ to be communicated to individuals concerned and the public at large, dependent on the seriousness and extent of the breach, which should be considered and implemented where appropriate.

5. EVALUATION AND RESPONSE

5.1 It is important that data breaches, actual or potential, are documented and investigated, and the response to the breach is evaluated in terms of its effectiveness.

5.2 Where a breach is caused by systematic and ongoing problems, merely containing the breach and continuing ‘business as usual’ will not be deemed acceptable. Areas requiring improvement for the purposes of preventing a re-occurrence should be identified and Policies and Procedures updated or implemented, as appropriate.

6. ADDITIONAL GUIDANCE

6.1 Additional guidance may be obtained from dataprotection@tscti.com

DATA BREACH INCIDENT REPORTING FORM

NAME OF PERSON REPORTING:	**DATE OF BREACH OCCURRING:TIME:**	**DATE ON WHICH BREACH WASDISCOVERED:** **TIME:**
DEPARTMENT:		
EXTENSION NUMBER:		
DETAILS OF THE DATA BREACH		
How did the breach occur?	*Please provide as much information as possible:*	
Has a breach of this natureoccurred before within theDepartment?	*If so, please provide dates of any previous breaches of the samenature:*	
How many individuals doesthe data breach affect?	*Please, aim to provide a figure as accurate as possible:*	

Are the individuals affectedby the breach staff?	
What data has been lost/stolen/compromised orelse disclosed without the appropriate authority?	*i.e. CVs, Financial Information, Contact details etc.:*
Whom was the data released to, if known?	
Is the data sensitive?YES/NO	*If YES, please provide a list of sensitive data concerned:*
Are you aware of theindividuals affected?	*If so, please provide their names and any contact details, whereknown:*
What steps could those individuals take to protectthemselves from any harm/risk arising from the breach?	*i.e. report to their bank/building society, report to the Police etc.:*
Does the breach concern manual or electronic data, or both?	
Were encryption protections in place at the time of the breach?	
Have the IT Services beeninformed?	*If your account has been hacked, you must change your passwordimmediately and report the incident to IT Services:*
Has the incident been reported to the Police orany other authorities?	*If so, please provide date of reporting and reference number:*
IS THERE ANYTHING ELSE THE ORGANISATION SHOULD BE AWARE OF?	
Please comment below:	
THIS FORM MUST BE SUBMITTED TO dataprotection@tscti.com and the Program Manager.	

When it comes to network traffic, it's important to establish a filtering process that identifies and blocks potential cyberattacks, such as worms spreading ransomware and intruders exploiting vulnerabilities, while permitting the flow of legitimate traffic. Latest in a series on best practices for network security, We explore best practices for network border protection at the Internet router and firewall.

Here are some principles to keep in mind:

- **Don't add an access control list (ACL) entry for every suspicious IP address.** The problem with this approach is that it creates a massive ACL. The Internet router now has to process every entry in the ACL when filtering traffic. This approach also makes it hard for people who manage the ACL, because network administrators must determine why a particular entry was added to the ACL, and whether that entry is still needed. Additionally, for devices that process an ACL in order from top to bottom, a longer and more complicated ACL makes it harder to be sure you've placed new entries in exactly the right place.

- **Protect the devices inside the border router and outside the firewall, and the outside interface of the firewall.** People often forget that there are vulnerable devices sitting outside the firewall, including the Internet router itself. There is usually no reason for someone outside your network to access the devices outside your firewall. It is important to have filters on the router to prevent unauthorized users from being able to log in to the router, or to send management traffic to the router.

  For devices between the Internet router and the firewall (like the switch in the diagram above), the easiest way to prevent access from the outside is to use non-routed RFC 1918 address space. A device with private addressing can't be reached directly from the Internet. That said, if you're protecting a network that already has public, registered addresses on internal network equipment (it happens), it's absolutely critical that you create ACL entries on your Internet router preventing access from the outside to your network equipment addresses. Remember to include the firewall's outside interface (if using public addressing on it) as well. If, for some reason, access to these devices is needed from the outside, you should permit only the specific source IP address and protocol needed.

  Out-of-band (OOB) management offers another option for reaching your border router, or other network equipment, from the outside. If you are using an external company to monitor your infrastructure, the external company should be able to provide you specific IP addresses and protocols. You can allow those and block everything else.

- **Filter the bogons.** The bogons list represents an entire class of private and reserved IP addresses.

  According to IT Team, which maintains the most up-to-date list of bogons, "a bogon prefix is a route that should never appear in the Internet routing table. A packet routed over the public Internet (not including over VPNs or other tunnels) should never have a source address in a bogon range. These are commonly found as the source addresses of DDoS attacks."

While we don't want to make the Internet router act as a firewall, the bogons list represents a simple way to eliminate obviously bad traffic at your network border, without the need for deep inspection, checking state tables, or complicated ACL entries.

If you're filtering bogons, however, it's important that you keep your filters up to date. The bogons list can change as previously unallocated IP addresses are allocated by the Regional Internet Registries (RIRs).

- Block inbound traffic sourced from your own IP addresses. At the Internet router, it is important to block any external traffic that is sourced from an internal IP address. For example, if you have your own allocated block of addresses, you should not see external traffic sourced from one of your internal addresses. If you see traffic sourced from your own internal IP space trying to enter your network from the Internet, it suggests either that someone is spoofing your addresses to try to do you harm or a routing problem has occurred. It is important to block this type of traffic at the Internet router because it is very possible that traffic allegedly sourced from your internal IP space is only subject to limited filtering once it gets to your internal network.

In summary, when considering filtering at the Internet router level

- Don't mess with intricate filtering systems to block every suspicious IP address.
- Focus on blocking bogons and anyone trying to spoof your IP addresses.
- Protect the Internet router from outside traffic, and protect anything that sits between the router and the firewall.

Let Firewalls Be Firewalls

At the firewall level, your approach to filtering should be more fine-grained. As with your border router, first and foremost it is important to lock down access to the firewall itself. Unauthorized users should not have access to this device.
In addition, there are two principles for filtering at the firewall level:

- **Default deny.** A firewall is a security device and is designed to protect your assets. Your default position when configuring the firewall should therefore be to deny traffic. Don't think of the firewall as the device that permits all traffic through, except for the things you want to block. Instead, think of your firewall as the device that blocks all traffic, except for those things you choose to permit.

- **Label everything.** With firewall filtering, it is important to assume that someday a new firewall administrator will have to figure out what you did and why. I have seen incredibly complex firewall rule bases that were hard to understand because the logic and reasoning behind them were unclear (e.g., IP addresses in rules with no indication of what devices the IP addresses represented, with no labeling to tell you why the traffic was being permitted or denied). When it comes to firewall filtering, every new rule should take into account that a future firewall administrator must one day read these rules and understand them.

When you are creating new rules to permit inbound traffic, try to be as specific as possible. For example, if you know a particular server requires inbound traffic on just three TCP ports, don't create a rule permitting all inbound TCP to that server--create a rule allowing only the needed ports. While it may be easier to make the rule less specific "in case we need to permit more ports later on," this opens up that server to all sorts of traffic that it shouldn't be receiving, including malicious traffic designed to exploit vulnerabilities on all those TCP ports you left open.

Sometimes when a new server or application is being brought online, I've seen people say "We aren't sure which protocols are needed--just permit everything for now and we'll lock it down when we know exactly what we need to permit through." In my experience, that later lock down never happens. Think carefully about whether you want to put a device on your network without knowing exactly which protocols it's supposed to be using, and then allow traffic on any protocol to reach it.

At the same time, while you're being as specific as possible with your rule set, there are best practices you can use to make it easier on yourself. If you create an object group in your firewall to include the IP addresses of all devices of the same type, with the same security requirements (e.g., all your web servers or all your email servers), you can create a single rule permitting all the specific ports and protocols needed to the entire group of servers at once.

Similarly, if there's a particular service on your network that you need to permit a known set of external IP addresses or networks to access, you can create an object representing all of those external addresses and networks, and then create a single rule allowing those external devices access to the needed service. Remember the rule about letting future firewall administrators understand what you did and why you did it? Label that object so it's clearly understood what those addresses represent (e.g., "External B2B Partners" or "Remote Office Admins"). Moreover, if you are able to add comments to your rules, add a comment that explains what the rule is for, and whether there is an expiration date for that rule.

Finally, it is important for the firewall administrator to conduct a regular--at the very least annual--audit of firewall rules. Ideally, you would have the documentation and rule change requests in one file to ensure an easier audit. Rule requesters should be asked to verify that the rule they requested is still required, and unneeded rules should be removed.

To recap, when it comes to firewall filtering, it is important to

- Ensure that your default position is to deny traffic, not to permit it.
- Label everything as specifically as possible.
- Conduct regular audits.

By taking a layered approach to network border filtering, you can block the most obviously bogus or potentially harmful traffic at your Internet router, while allowing the firewall to do what it's designed to do, and inspect and block the remaining threats.

Review and Revision

The Environmental Control Guidelines will be reviewed and revised in accordance with the Information Security Program Charter.

Recommended: ________________________

Signature

Pakkirisankar Jagannath

Program Manager

Approved: ____________________________

Signature

Anil Sharma

CEO