CYBER SECURITY INCIDENT RESPONSE PLAN (CSIRP)

1. Table of Contents

2. Doc Info

Revision history

Classification	
VERSION	3.9 (redacted version)
Effective Date	05/23/2024
DOCUMENT AUTHOR	
DOCUMENT OWNER	

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

Approval

Name	Position	Signature	Date

3. Overview and Purpose

The purpose of this document is to provide guidelines for teams responding to incidents at their organization. The plan that follows provides guidance and suggests documents that should be created in order to respond to incidents properly. It provides roles and responsibilities of Incident Response Team members and suggests steps that should be considered for each phase of Incident Response. In some instances, additional steps and actions may be required which are not included in the attached document. All members should use their professional judgment when addressing a Cyber Security Incident.

This IR Plan applies to all TrueBlue's IR Stakeholders responding to cyber security incidents involving TrueBlue's information technology systems.

4. Introduction

TrueBlue's IT/Data/Cyber Security personnel/department manages a wide variety of security challenges, but the most threatening of these (cyber security incidents) have the ability to damage data and/or processing resources resulting in the potential loss of business and/or interrupting business operations. To deal with such threats in a consistent and structured manner, TrueBlue has created the framework described in this Cyber Security Incident Response Plan (CSIRP). This plan is intended to provide an enterprise-level management strategy for the corporation, addressing incidents both proactively and, when necessary, reactively.

A Data/Cyber Security incident is a compromise, attempted compromise, or suspected compromise of the confidentiality, integrity, or availability of information or information systems from any cause or a violation of information security policy. Some examples of incidents that can be managed within this plan include network intrusion, denial of service (DoS), DNS attacks, malware (virus, trojan, or worm) infection, internal misuse of information systems resources, phishing emails, and advanced persistent threats (APTs). Also, investigation of data loss due to the physical loss of computing or networking equipment is within the scope of this plan. Still, TrueBlue Facilities handles physical security and is responsible for preventing and prosecuting the actual physical loss.

The plan is focused on protecting TrueBlue's information systems assets. However, preventing incidents can extend the scope of attention to public networks (especially the Internet) to which TrueBlue's network is connected.

5. Disclaimer

This plan was created based on NIST 800-61, best practices from industry, and experienced consultants. This plan should be viewed as a guideline and is not guaranteed to be the exact and only steps that TrueBlue should take in the case of any incident.

6. Goals

- The CSIRP maintains a consistent structure in TrueBlue's global response to each cyber security incident.

This structure achieves the following objectives:

- Defines key roles and responsibilities for incident handling participants
- Identifies external threats with the potential to generate cyber security incidents
- Minimizes the time needed to identify information security incidents
- Identifies preventive controls for protecting TrueBlue resources from future external threats
- Reduces disruption to business operations during incident response
- Protects data integrity during evidence collection
- Minimizes overall recovery time
- Establishes proper external communication to avoid negative publicity and to meet legal, regulatory, and contractual obligations
- Develops internal communication to provide information to those involved in identifying, analyzing, and responding to incidents; and develops internal communication to technology management, business line management (as appropriate), Corporate Counsel, Security personnel/department, and others, as necessary
- Protects TrueBlue from litigation or adverse legal judgment in response to improper investigative procedures
- Provides investigative support for potential legal response to incidents
- Provides a system for tracking incidents
- Provides feedback to the Security Awareness Program on incidents that may have been avoided with heightened employee security awareness

7. Team Member & Communication Lists

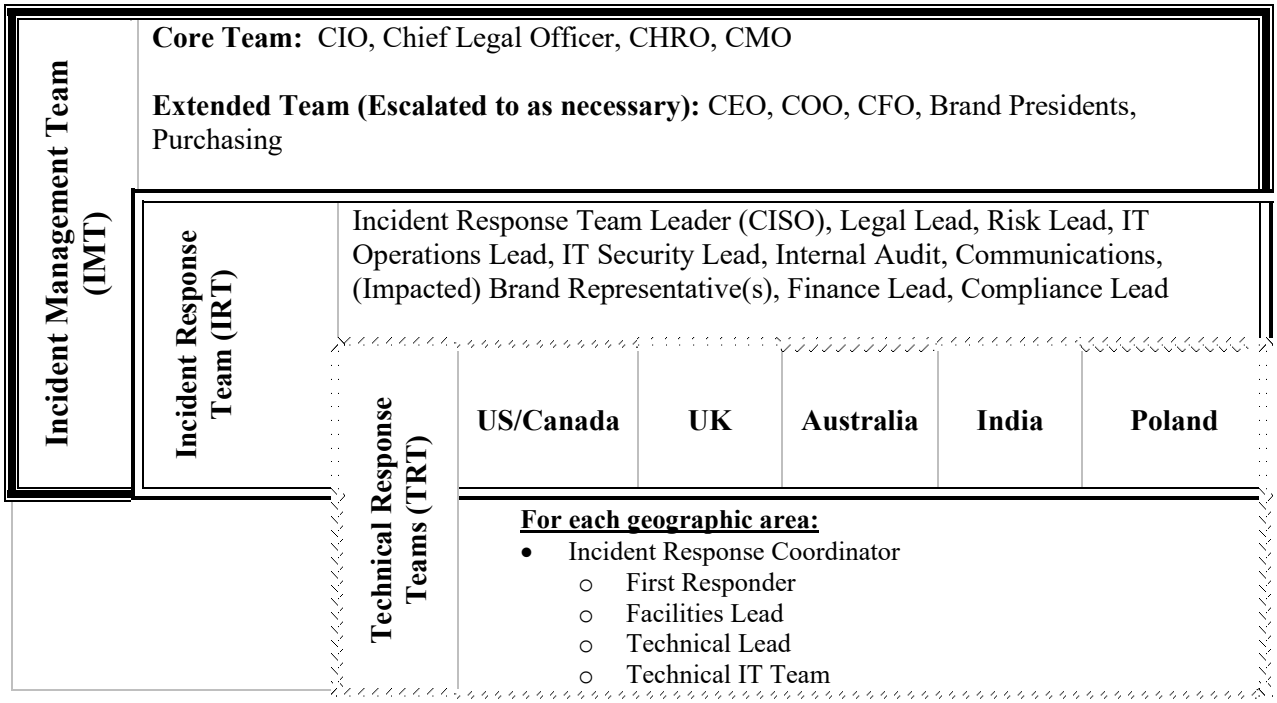
The Cyber Security Response consists of three response teams:

Incident Management Team (IMT): These are the executive members who make key business decisions and determine communications regarding incidents that reach that level of attention.

Incident Response Team (IRT): The Incident Response Team (IRT) represents the Information Technology (IT) experts employed by TrueBlue. They coordinate IT and other resources necessary to bring the company back to pre-incident operational capabilities.

Technical Response Team (TRT): The Technical Response Team (TRT) is TrueBlue's first line of Information Technology experts. They identify and investigate cyber incidents to assess their impact on the organization and determine the most effective and proper way to resolve the issue.

Incident Communications Team (ICT): The Incident Communications Team (ICT) provides stakeholders with timely, accurate, and consistent communication to internal and external stakeholders.



ALL TRUEBLUE EMPLOYEES, whether they have a role within this plan or not, must report cyber security incidents or anomalies. This requirement will also be reinforced in the awareness training that all employees receive.

5.1 Incident Management Team (IMT)

Name	Title/Role	Office	Cell	E-Mail	Location

5.2 Incident Response Team (IRT)

Name	Title/Role	Office	Cell	E-Mail	Location

5.3 Technical Response Teams (TRT)

Name	Title/Role	Office	Cell	E-Mail	Location

8. Incident Alert Hotlines

Personnel may contact the Incident Response Team using the following hotlines. The hotlines will be posted to all personnel, so they know how to contact the Incident Response Team.

Incident Alert Hotlines	
Hotline Method	**Contact Information**

9. Incident Response Experts/Additional Contacts

The following authorities will be called in case of a data breach incident or a system breach incident.

Incident Response Experts		
Role	**Party**	**Contact Information**

10. Interested Parties Contacts

In the event of a data breach incident or a systems breach incident, Senior Management to contact the below persons need so that they can provide the business with a high-level summary of how to ensure pertinent interested parties are identified and communicated to in the event of an incident.

Name	Title	Phone	Email

11. Team Responsibilities

Please reference document TBI_Incident Response Plan_2023 - Ancillary - Roles and Responsibilities.docx for complete list and description of Roles and Responsibilities.

12. Principles regarding this plan

1. **Record all notes on paper.** Do not record incident or event information into a computer system that is on a compromised network. Record all notes on paper. Templates for note taking are provided in this plan.
2. **Manage Public Announcements.** Attackers must not become aware of their victims' reaction to their attack. Premature and incorrect announcements to the public about the nature of an incident can be unnecessarily harmful.
3. **Use the Cyber Incident Response Plan for all incidents**. Breach Incidents will result in investigations from outside parties and authorities.

Minimize use of acronyms/brevity codes. When in meetings, or in communications, be sure to fully write out or fully state the words for all acronyms or short codes to avoid any confusion during a stressful time. Key Terms Defined

13. Incident Categories

13.1 Security Event

Failure or violation of a control with no impact:

- Relatively common with a high level of regular occurrences
    - Port scans against websites
    - Spam and phishing emails
    - Failed password number of attempts

13.2 Cyber Security Incident

A security event with an impact that must be investigated and resolved:

- May be predicated by numerous seemingly unrelated security events
- Can vary in magnitude of impact to the organization
- Possibly will require external notification
    - In the event that external notification is required, data custodians, government and regulatory bodies and other necessary parties will be notified in a reasonable timeframe, and in compliance with regulatory and other applicable requirements and guidance

14. Types of Incidents

There are TWO types of INCIDENTS:

14.1 Operational Incident

- A critical failure / unstable condition of a system, application, or network
- Significant effort may be required to recover from an Operational Incident
- A system may have failed to operate, be damaged / broken, or otherwise be operating in an abnormal or unauthorized manner
- Handled by Cyber Security Operations function

14.2 Cyber Security Operations functions

- Simplify operations by integrating and consolidating tools
- Automate repetitive tasks to better use your analyst talent
- Consistently enforce policy across networks, clouds, and endpoints
- Rapidly respond to threats with deep visibility and contextual insight
- Infrastructure security including but not limited to:
    - Network Security
    - Cloud Security
    - Access Controls
    - Whitelisting
    - Perimeter Security
    - Data Privacy
    - Security Monitoring
    - Policy Management

14.3 Cyber Security Incidents

- A critical compromise to a system or application.
- A breach involving sensitive information exposed to unauthorized individuals (Protected Health Information (PHI), Personally Identifiable Information (PII), credit card data etc.).
- The impact involves external parties and is generally caused by illegal activity.
- This may require disclosure and cooperation with legal authorities.
- Outside involvement (investigators, regulatory agencies, law enforcement agencies, attorneys etc.) will likely be required in a breach situation.
- Handled by Cyber Security Incident Response Team

14.3.1 Cyber Security Incident Response Team Functions

- Identification of Threats
- Detection of Threats
- Visibility of Threats
- Isolation and Containment of Threats
- Eradication of Threats

- Threat Intelligence
- Process Workflows and Automation
- Integration of Tools
- Collaboration and Information Sharing

14.3.2 Examples of Cyber Security Incidents

- Malware: Software designed to disrupt or obtain illegal access to computer systems or networks, such as viruses, worms, Trojans, ransomware, and spyware.
- Phishing: Uses fraudulent techniques, usually via emails or websites, to fool people into disclosing sensitive information such as passwords, credit card information, or personal information.
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS): DoS attacks flood a target system with excessive traffic or resource demands, leaving it inaccessible to normal users. Multiple sources are used to coordinate DDoS attacks.
- Data Breaches: Unauthorized access or disclosure of sensitive information, such as personal records, financial data, or intellectual property, through targeted attacks or system flaws.
- Insider Threats: Sabotage, data theft, or illegal access by those who have legitimate access to systems or networks, such as employees, contractors, or partners.
- Social engineering: Manipulation tactics used to deceive or acquire the trust of others in order to get sensitive information or persuade them to perform acts that benefit the attacker.
- Zero-day exploits: Exploiting flaws in software or hardware that are unknown to the vendor or do not have updates available, allowing attackers to gain unauthorized access or control.
- Advanced Persistent Threats (APTs): Long-term, targeted attacks carried out by highly competent and motivated adversaries who acquire illegal access to networks, create a persistent presence, and remain stealthy in order to steal critical information or monitor activities.
- Insider attacks: Attacks carried out by individuals with authorized access to systems or networks who abuse their rights for personal gain, vengeance, or other nefarious reasons.
- Physical attacks: Include theft, destruction, or tampering with hardware components, as well as physical damage or unauthorized access to computer systems, networks, or infrastructure.

15. The Tools and Technologies that support the Security Program:

- Palo Alto Firewalls – Access Controls, Whitelisting, Perimeter Security, Policy Management
- Palo Alto Panorama – Console view of all Firewalls in all datacenters
- Imperva -Web Application Firewalls and Database Monitoring
- Rapid7 -Vulnerability Scanning
- Okta – Single Sign-On and Multifactor Authentication
- CyberArk – Privileged Access Management and Local Administration Vaulting
- PagerDuty – Incident and Event Monitoring
- Microsoft Identity Manager – On-boarding and Off-boarding employees and contractors
- Proofpoint – Targeted Attack Protection, Threat Response Auto Pull, Internet Mail Defense, Email Fraud Defense, Cloud Access Security Broker
- Palo Alto XDR– Endpoint Detection Response
- Red Canary – Managed Detection Response, Security Orchestration Automation Response, Managed Service Security Operations Center

Security Operations and Cyber Security Incident Response Management is 24x7x365 supported by On-Call Rotation for all members of the Cyber Security Operations Team. All Change Controls rules are followed, and all upgrades, patching and configuration management are adhered to through an organized Change Management Board.

16. Cyber Incident Severity Escalation Matrix

Whether an event or an incident, the severity of the situation must be addressed and communicated. The matrix below guides the incident response teams to determine the severity and when to activate the appropriate team.

Cyber Incident Severity Classification & Escalation Matrix			
	Level 1 Guarded	**Level 2 Elevated**	**Level 3 Severe**
Definition	Minimal impact on operations and/or security	Significant impact on operations and/or security	Severe impact on operations and/or security
Examples	- Isolated virus infections - Unauthorized access attempts - External scans / probes / attempted access - Attempts to exfiltrate sensitive information - Denial of Service attempts	- Malware outbreak - DoS attack - Internal scans / probes / attempted access - Deny availability to a key system or service	- Enterprise wide malware outbreak - Unauthorized access to critical systems - Enterprise wide DDoS attack - Network disruption at critical locations - eCommerce website compromise causing outage - Whaling Email attack
Impact Types	**Level 1 Guarded**	**Level 2 Elevated**	**Level 3 Severe**
Information Impact (Software, Network, Database, and Access)	No information was exfiltrated, changed, deleted, or otherwise compromised	- Limited anomalies in monitoring and processing patterns. - Multiple suspicious and possibly related tickets opened. - Operational anomalies noted in systems or data	- **Privacy Breach** Sensitive PII of clients or employees breached - **Proprietary Breach** Unclassified proprietary information, potential critical infrastructure information PCII was accessed or exfiltrated - **Integrity Loss** Sensitive proprietary information changed or deleted
Brand & Reputation (Traditional and Social Media)	Routine comments regarding Company	- Multiple postings regarding operational difficulties	- Brand attack on Company - Cyber action reported - Employee/Client data posted on internet - Loss of PII or PHI reported - Company problems reported - Public awareness of hack

Functional / Operational Impact (Customer experience, Internal/External)	No or minimal impact on organization ability to operate	- Organization has lost the ability to provide a critical service to a subset of internal or external customers - Business processes and/or functions have degraded or controls are not functioning as designed	- Organization is no longer able to provide some critical services to any users - Loss of revenue
Data Recovery (Time, Effort, Ability)	Time to recover is predictable and minimal	- Time to recover is predictable with additional resources - Time recovery is unpredictable; additional resources and outside help are needed - Data appears to be corrupt, inaccurate or is not current	- All data lost - Data missing/manipulation - Inability to access information - Recoverability not possible - data exfiltrated and posted publicly - Launch investigation
Enterprise Support Actions	**Local Security Team** **TRT leads response**	**Refer to IRT /notify ICT** **TRT Leads Response**	**ESCALATE to IMT** **TRT Leads Response**

17. Incident Response Plan Lifecycle

Regarding this plan, most, if not all of the steps listed below will occur BEFORE this plan is activated. The steps below describe what would generally happen to activate this plan. The Status column is there to check off what steps happened.

To ensure swift and efficient handling of security incidents, we have established internal Service Level Agreements (SLAs) as part of our comprehensive Incident Response Plan. These SLAs outline the time-bound objectives and responsibilities of our incident response teams, aiming to minimize the impact of security events and maintain the confidentiality, integrity, and availability of our assets. All Cybersecurity Internal SLA's can be found in the "TBI Incident Response - Ancillary - Internal Service Level Agreement.docx" document.

17.1 Alerting

Description

The alerting phase of incident management begins with a trigger that activates human intervention to determine whether the trigger indicates a genuine incident. Incident detection can be triggered by various sources, which TrueBlue describes in five categories:

- External notification
- Alerts from a preventive system

- Log review detection
- Compliance Monitoring
- User report of suspect activity

External Notification

The Incident Response Team (IRT) or other designated qualified trained staff receives automated notification of security threats and vulnerabilities from security vendors and organizations. IRT staff also monitor online alert services. Any notification rated as critical by the notification source is evaluated as a possible incident. This process typically addresses the public discovery of a new threat, such as malware, or a previously unknown software vulnerability, which may not yet have affected TrueBlue's systems.

Alert from Preventive System(s)

All of the technical controls that play a role in the prevention of incidents within TrueBlue are configured to generate alert messages if certain types of events (such as network traffic matching a defined worm signature) occur, or if activity passes a predetermined threshold (DDoS detection, for example). Intrusion Detection System (IDS) alerts and other protective system alerts are initially directed to SOC/MSOC for initial review, triage, and prioritization; alerts identified as potential cyber security incidents are directed by the designated notification system to the IRT On-Call.

Log Review Detection

Alerts based on logs of domain controllers, servers, and other systems are reviewed by the System Administrators and Security personnel/department. Unauthorized activity is reported to IRT and anomalous activity is reviewed by the SOC/MSOC for potential security threats or incidents. Those determined to be threats or cyber security incidents are forwarded to IRT.

Compliance Monitoring

Assessment service vendor(s) or internal, qualified, trained staff perform regular assessments of the "security health" of TrueBlue systems. These include penetration tests, vulnerability assessments, baseline comparisons, web-based application assessments, and wireless assessments. Any of these assessments may uncover a threat that, dependent on the circumstances, might escalate to cyber security incident status and be reported to the IRT On-Call.

User Report of Suspect Activity

When employees notice activity that they suspect indicates an attempted intrusion or violation of security policy, the IT Service Desk should be contacted, which, in turn, will contact the IRT On-Call.

It should be noted that multiple triggers are a strong sign that a genuine incident has occurred. Often, a true incident trips alarms in more than one preventive system. For example, malware is frequently detected by antivirus software on email gateways as well as IDS systems.

Detailed Guidance:

#	Task	Responsible Team(s)	Status
A-01	A ticket has been created and is being reviewed by the support team	User/Event	
A-01a	Alerts from a preventive system triggers an "alert" email or page – Enters a ticket reflecting alert.	Technical Monitoring Team	

A-02	Support Desk Team member suspects security event/incident escalate to the "1.5 team or Level 2."	Support Desk	
A-03	Determine that this is an incident, escalate to Technical Lead	"1.5 Team" or Level 2	
A-04	Technical Lead reviews, determines whether or not warrants escalation to Triage	Technical Lead	
A-05	Technical Lead alerts rest of local Incident Response Team to begin Triage.	Technical Lead	
A-06	Technical Lead notifies Incident Response Team that Triage is being done on an event/incident (AWARENESS)	Technical Lead	
A-07	Technical Lead notifies other Local Incident Response Teams (AWARENESS)	Technical Lead	
A-08	Triage begins	Technical Response Team	

17.2 Triage

Description:

The goal of Triage is to gauge the size and shape of an incident, and to validate that it is indeed an incident, based on clear criteria. While there may be some immediate, obvious actions that can take place, the key is to maintain clear communication before any measures that can have wide-ranging impacts.

Upon Exit of Triage – The team should determine:

1) Classification of Incident (Event, Operational or Cyber Security Incident)
2) Security Level of Incident
3) Initial Response
4) Then – decide whether or not this plan should continue

Detailed Guidance:

#	Described	Responsible	Status
T- 01	**Form Technical Response Team (TRT)** Depending on where the incident was discovered, the local incident response team will take the lead in beginning Triage	Technical Response Team	
T-02	**Begin Triage** • Identify the Scene • Protect the Scene • Collect complete information about the incident • Document Observations and Actions **Document all observations and actions:** • ***Form Used:*** *Observations and Actions* **Document inventory of all impacted assets:** • ***Form Used:*** *Inventory of Impacted Assets*	First Responder Technical Response Team	
T-03	**Classify Incident** • Event • Operational Incident • Cyber Security Incident • ***Form Used:*** *Incident Classification Form* **If a Cyber Security Incident, maintain evidence control:** • ***Form Used:*** *Chain of Custody Form*	Technical Response Team	
T-04	**Assign Security Level** Using the Cyber Incident Severity Escalation - Guarded - Elevated - Severe	Technical Response Team	
T-05	**Determine initial response approach** **While there may be some immediate obvious actions, the key is to determine an approach.**	Technical Response Team	

#	Described	Responsible	Status
	If the incident is active or on-going, begin immediate action to contain and control the incident by securing and blocking unauthorized access to systems/data and preserve evidence for investigation. Related actions may include (but not be limited to): • Shut down particular applications or third party connections; • Isolate (preferred) or shut down (when no other options exist) hardware; • Reconfigure firewalls; • Change computer access codes; and/or • Modify physical access controls Note: Consequences to systems and business services availability must be weighed against immediate risk exposure before taking such actions without first consulting the IRT ***Form Used:*** *Response Approach (investigation/containment)*		
T-06	**Communicate to IRT** Communicate situation to IRT, who may in turn communicate to higher teams as necessary Use the Cyber Incident Severity Escalation Matrix and/or Escalation Criteria guide below to assist in determining the appropriate initial assessment. If any of the items on the Escalation Criteria are met, then communication ins mandatory	Local Incident Response Coordinator	
T-07	**DECISION: Continue Investigation?** If the incident meets the criteria for Classification, and Security Level, then continue investigation, or else handle through normal departmental procedures. **Contact Third Parties as necessary:** • ***Form Used:*** *Third Parties Contacted*	IRT	
T-08	**Complete necessary paperwork** Complete all forms as directed by this plan. Forms are listed above and here in summary: • **Observations and Actions** • **Inventory of Impacted Assets** • **Incident Classification Form** • **Chain of Custody Form** • **Response Approach (investigation/containment)** • **Third Party Contact Form**	IRT Incident Response Coordinator ensures this is done.	

Use this as additional guidance to determine whether or not to communicate to the IRT.

Escalation Criteria Guide	
Criteria	**Example**
Customer related data is compromised (confidentiality and integrity) in any way, including vendors that maintain company data	• Data seen on the internet • Employees know that they sent protected data to unauthorized person on accident • Employee lost unencrypted laptop with confidential data on it • Confirmed that confidential data was exposed to unauthorized people
It is confirmed that automated alerts are beyond normal operating levels, for unacceptable known or unknown reasons	• Many alerts of the same type • Alerts of various types in a narrow timeframe
There is a confirmed pattern of unexpected customer reports of various issues in a narrow timeframe	• People calling in about the system being "down" • Calls "reported" from the company that were not from the company • Phishing emails • System behaving unexpectedly
It is clear that a law or regulation has been violated	• Exposure of confidential data • Sensitive documents have been incorrectly sent to incorrect people

Incident Classification Guidance

Incident Classification	Defined (definitions are considered to be "OR" statements – not "AND" statements. Any of the below can be true for the classification to be correct.)
Security Event	Failure or violation of a control with no impact.
Operational Incident	System failure causing impacts to data confidentiality, integrity or availability A critical failure/unstable condition of a system, application, or network. - system may have failed to operate, be damaged/broken, or otherwise be operating in an abnormal or unauthorized manner "Forensic analysis" is generally not needed External communication to customers and/or authorities is generally not needed.
Cyber Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices Intentional or accidental policy violation by internal staff that impacts confidentiality, integrity, or availability of a system, network or application Will most likely require "forensic analysis" of incident Will most likely result in communication to customers and other stakeholders

Incident Classification	Defined (definitions are considered to be "OR" statements – not "AND" statements. Any of the below can be true for the classification to be correct.)
	A Cyber Security Incident is a critical compromise to a system or application, which involves sensitive information exposed to unauthorized individuals, data changed by unauthorized individuals, or availability of systems impacted by unauthorized individuals Could involve external or internal parties, but generally caused by illegal activity in either case May require disclosure and cooperation with legal authorities Outside involvement (investigators, regulatory agencies, law enforcement agencies, attorneys etc.) will likely be required in a cyber security incident

17.3 Investigation

Description:

Depending on the type of incident, an incident response member from the appropriate Technical Response Team (possibly multiple) will be responsible for analyzing the incident.

In the process of answering the bigger questions such as determining the incident classification, questions that need to be asked/answered within this phase are:

1) What is the overall scope of the incident?
2) How many users impacted?
3) What is the type of data impacted?
4) What type of systems are impacted – and are "neighboring" systems likewise affected?
5) What type of technology is impacted – and what other systems use that same technology?

While the above questions are important, they will inform the bigger questions such as Incident Classification, and Obligation Notification, as is described in the detailed steps below.

Detailed Guidance:

#	Described	Responsible	Status
I-01	Confirm/Approve Incident Classification • ***Form Used:*** *Incident Classification Form*	Coordinator IRT Leader	
I-02	Confirm/Approve Response Approach This can be in a course of a meeting between teams, and the incident is escalated to the IMT is escalated to if the response approach has a large impact to production systems. ***Form Used:*** *Response Approach (investigation/containment)*	Coordinator IRT Leader IMT Leader (if escalated)	
I-03	• Deploy first responders to impacted assets to collect evidence and complete Impact Assessment Form ***Form Used:*** *Impact Assessment*	Technical Response Team	
I-04	**Execute Investigation** • ***Form Used:*** *Response Approach* **Document all observations and actions:** • ***Form Used:*** *Observations and Actions* **Document inventory of all impacted assets:** • ***Form Used:*** *Inventory of Impacted Assets* **If a Cyber Security Incident, maintain evidence control:** • ***Form Used:*** *Chain of Custody Form* **Consider these steps:**	Technical Response Team	

#	Described	Responsible	Status
	• Gather information about any scheduled and/or emergency system(s) changes or maintenance during the time surrounding the event • Question team members and employees who may have ancillary information pertaining to the incident (i.e. on-call support staff, affected users, system/data owners, etc.) • Identify any essential elements of information that would escalate the severity of the incident (i.e PII, PCI, or HIPAA data/assets involved in suspected incident) • Query any Third parties that may have data pertinent to the investigation (this could include Third party service providers, vendors, web hosts, etc.) • Attempt to identify any internal assets that were used to launch or facilitate the attack • Deploy First Responders and/or allocate additional resources to aid in investigation, as necessary • As information on the suspected incident becomes available, use key indicators of compromise to assess the nature of the attacker and their level of sophistication. Use this information to assess how the attack will likely progress • Use Open Source Intelligence (OSINT) gathering techniques to find patterns or indicators that could aid in identifying the likely attacker and their motivations. This will help identify other key areas of interest in the investigation.		

I-05	**Determine Obligation Notification (Breach) Classification**
	
	Based on the evidence presented by the Technical Response Team, determine the notification classification:
	• **NO BREACH**
	  ○ We are certain there was no breach.
	• **BREACH UNLIKELY**
	  ○ There is no reason to believe that a breach occurred.
	• **REASONABLE BELIEF THAT A BREACH OCCURRED**
	  ○ A breach was possible, but we may not have proof.
	• **BREACH**
	  ○ We are certain that the disclosure occurred, unauthorized persons had access to data, and did cause harm.
	• **CONTAINED DISCLOSURE**
		IRT	

#	Described	Responsible	Status
	○ Unauthorized persons acquired information, but we are certain that the disclosure is contained and will not create harm.		
I-06	On reviewing the Breach Classification: • Communicate to parties outside the company as necessary, based on obligations or laws.	IMT	
I-07	• Contact Third parties, based on recommendations from technical teams if they need expert assistance. Inform ICT of these contacts. ***Form Used:*** *Third Parties Contacted* • Communicate to employees within the IT Teams as necessary.	IRT	
I-08	• Necessary communication to internal or external parties regarding the incident.	IMT, ICT	
I-09	**Complete necessary paperwork** Complete all forms as directed by this plan. Forms are listed above and here in summary: • **Observations and Actions** • **Inventory of Impacted Assets** • **Impact Assessment** • **Incident Classification Form** • **Chain of Custody Form** • **Response Approach (investigation/containment)** • **Third Parties Contacted** • **Status Meeting Minutes (used for any meetings)**	Technical Response Team IRT Incident Response Coordinator ensures this is done.	

17.4 Containment

Description:
Once the incident has been detected and analyzed, it must be contained before it spreads. The goal is to "stop the bleeding." Before anything can be ultimately fixed, the breach needs to be closed (or whatever the situation may be). The containment approach may have been initially created in the Triage and Investigation steps as part of the overall response approach; it is confirmed and carried out in this step. Confirm a containment approach and enable the appropriate team members to execute.

Containment is a process by which information, architecture, and/or system configurations are modified to reduce the emergent risk to TrueBlue's assets. Types of containment or mitigation procedures which the team may consider include, but are not limited to:

- Isolate impacted system from the rest of the network
- Block specific ports through firewall(s)
- Disable Internet email
- Apply vendor-supplied patch or configuration changes
- Modify ACLs on systems or firewalls
- Shut down VPN access to TrueBlue internal systems
- Change passwords or block accounts used for unauthorized access
- Shut down or isolate affected systems
- Adjust DDoS policy settings on the DdoS detectors
- Block source IP addresses for malicious traffic
- Block destination IP addresses in case of a botnet
- Implement more aggressive policies, where applicable

Implemented changes should be broad enough to control further compromise, yet as granular as possible to limit the impact on legitimate business activity. Some containment strategies (especially those involving system shutdown or disabling a service) will be implemented on a short-term basis, until threats can be permanently eradicated. Ideally, containment procedures eliminate further threat without further negative impact or reducing system functionality.

The IRT should have representation from the groups that will deploy containment procedures, such as the System Administrators, Application, and IT Service Desk. Unless confidentiality concerns prevent it, any containment methods should be implemented by staff normally responsible for changes to the affected systems.

Evidence Handling

Clearly document how all the evidence has been preserved.

- Evidence should be accounted for at all times. Whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature.
- A detailed log should be kept for all evidence, including the following:
  - Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer)
  - Name, title, and phone number of each individual who collected or handled the evidence during the investigation
  - Time and date (including time zone) of each occurrence of evidence handling
  - Locations where the evidence was stored

Detailed Guidance:

#	Task	Responsible Team(s)	Status
C-01	• Determine/Confirm Containment Approach • Gain approval from IRT ○ ***Form Used:*** *Response Approach (Containment)* Some of the criteria for incident containment that should be considered are: • Potential damage to and theft of resources • Need for evidence preservation • Service availability • Time and resources needed to implement the approach • Effectiveness of the approach (partial or full containment)	Technical Response Team	
C-02	• Review and Approve containment approach ○ ***Form Used:*** *Response Approach (Containment)* • Escalate to IMT as necessary Any decision to disconnect or shut down a system should be made with careful consideration of the resulting impact on critical systems and services, and with appropriate communication to affected system owners, users, and business owners	IRT/ICT	
C-03	If escalated, review and approve containment approach. ○ ***Form Used:*** *Response Approach (Containment)*	IMT	
C-04	**Test Containment Approach** • New or unrelated problems or undesired business impact(s) may arise as a result of any changes made to contain an incident • All procedures and alterations performed must be thoroughly documented by the IRT and tested, whenever feasible, in a non-production environment, according to established procedures ***Form Used:*** *Response Approach (Containment)*	Technical Response Team	
C-05	Upon a successful test: Begin executing the selected containment approach: • Enable the Network, Database, System, Application and Special Interest teams to effectively respond to the threat by making swift, informed decisions and providing clear guidance to the team members • Information gathered for troubleshooting and as evidence should be collected according to procedures that meet all applicable laws and regulations ***Form Used:*** *Response Approach (Containment)* **Document all observations and actions:** • ***Form Used:*** *Observations and Actions* **Document inventory of all impacted assets:**	Technical Response Team IRT (if necessary)	

#	Task	Responsible Team(s)	Status
	• ***Form Used:*** *Inventory of Impacted Assets* **If a Cyber Security Incident, maintain evidence control:** • ***Form Used:*** *Chain of Custody Form*		
C-06	• Contact Third parties, based on recommendations from technical teams if they need expert assistance ***Form Used:*** *Third Parties Contacted* • Communicate to employees within the company (as necessary; on a limited basis). o Example - Send out user-level instruction to prevent the spread of the infection with CMIT approval	IRT	
C-07	• Communicate to employees within the company as necessary. o Example - Send out user-level instruction to prevent the spread of the infection • Communicate to parties outside the company as necessary	IMT	
C-08	**Complete necessary paperwork** Complete all forms as directed by this plan. Forms are listed above and here in summary: • **Observations and Actions** • **Inventory of Impacted Assets** • **Incident Classification Form** • **Chain of Custody Form** • **Response Approach (investigation/containment)** • **Third Parties Contacted** • **Status Meeting Minutes (used for any meetings)**	Technical Response Team IRT Incident Response Coordinator ensures this is done.	

17.5 Eradication

Description:

The goal of the eradication effort is to eliminate any traces of the incident.

Eradicate the incident

- Eliminate the cause/effect of incident
- Identify and mitigate all vulnerabilities that were exploited
- Remove malware, inappropriate materials, and other components
- If more affected hosts are discovered (e.g., new malware infections), repeat the previous steps to identify all other affected hosts, then contain and eradicate the incident for them

During this process a suitable eradication approach is created and reviewed. Industry best practices and the disaster recovery plan will be considered while developing an approach. Eradication may involve locating systems that are infected and cleaning each of them completely to regain control.

Eradication processes are intended to remove an intrusive agent (e.g., malicious code) from a compromised system, and to eliminate the possibility for future occurrences of the same incident. In some cases, these goals will be completed within the containment phase of incident management. Eradication is a necessary secondary activity when temporary, and possibly, incomplete containment procedures were put in place to block the immediate impact of a threat. Some of the same types of procedures implemented for containment may be used for eradication. In addition, other measures may be considered, such as:

- Patching systems not immediately considered vulnerable
- Implementing physical security controls
- Removing malware from affected systems
- Isolating systems or subsystems
- Cleaning infected systems

Detailed Guidance:

#	Task	Responsible Team(s)	Status
E-01	Determine Eradication Approach – submit for approval • ***Form Used:*** *Response Approach (eradication)*	Technical Response Team	
E-02	Approve Eradication Approach • ***Form Used:*** *Response Approach (eradication)* Escalate to IMT as necessary	IRT	
E-03	If escalated, review and approve eradication approach. • ***Form Used:*** *Response Approach (eradication)*	IMT	
E-04	**Execute Eradication Approach** • ***Form Used:*** *Response Approach (eradication)* **Document all observations and actions:** • ***Form Used:*** *Observations and Actions* **Eradicate all impacted assets:** • ***Form Used:*** *Inventory of Impacted Assets*	Technical Response Team	

#	Task	Responsible Team(s)	Status
	If a Cyber Security Incident, maintain evidence control: • ***Form Used:*** *Chain of Custody Form* • Restore Assets to known good state • Return affected systems to an operationally ready state • Confirm that the affected systems are functioning normally If necessary, implement additional monitoring to look for future related activity		
E-05	Contact Third parties, based on recommendations from technical teams if they need expert assistance. • ***Form Used:*** *Third Parties Contacted*	IRT	
E-06	• Communicate to employees within the company as necessary. • Communicate to parties outside the company as necessary.	IMT	
E-07	**Complete necessary paperwork** Complete all forms as directed by this plan. Forms are listed above and here in summary: • **Observations and Actions** • **Inventory of Impacted Assets** • **Chain of Custody Form** • **Response Approach (eradication)** • **Third Parties Contacted** • **Status Meeting Minutes (used for any meetings)**	Technical Response Team IRT Incident Response Coordinator ensures this is done.	

17.6 Recovery

Description:

In recovery, the "emergency" aspect of the incident is now over. It is it time to figuratively "sweep up." The systems have been restored to a known good state, now it is time to recover and see what happened, and why. We also need to make sure those that were harmed are "made whole," as well as start to improve our systems.

Restore System to Secure State

Recovery is intended to return systems and services to functionality. In some cases, this may/may not be identical to their original state if alterations have been made due to data loss or to eliminate vulnerabilities.

Depending on containment and eradication procedures used, systems may be off-line or operating with limited functionality. These systems must be returned to full operation as soon as it can be securely and safely done; additional monitoring tools or procedures may be put into place at this time. If data loss occurred with the incident, it must be restored as fully as possible.

Systems must be evaluated both for functionality and secure operation before being returned to production.

Review and update general recovery strategies, considering:

- Stakeholder impacts
- Expected outage duration of essential services
- Any special security, and operational issues or concerns related to:
  - Clients
  - Employees
  - Client Employees
  - Associates
  - Subsidiaries
- Any special insurance issues or concerns
- Any special regulatory issues or concerns
- Any special international operation or regulatory concerns
- Any special traditional and/or social media-related concerns
- Contact status for all recovery personnel
- Potential short-term corrective action, if possible and
- Estimated time to be recovered
- Internal communications for response notifications
- Role of law enforcement
- Notification appropriate teams that incident is complete, if the event has concluded

There are a number of considerations regarding recovery, some of them are listed below:

- If the incident represents a threat to affected individuals' identity security, consider remediation measures to mitigate the risk of negative consequences for those affected:
  - Credit monitoring services
  - Credit freeze
  - Identity theft insurance
  - Identity theft help information packets/letters
  - Compensation for identity theft
- Consider litigation matters that may arise, including;
  - Civil lawsuits instituted by affected persons against the company or the company subsidiaries

    - Investigation of TrueBlue/TrueBlue subsidiaries and/or specific employees by law enforcement authorities
    - Indemnification by third parties in the event that third parties are at fault for data security cyber action
- Compliance:
    - Keep all regulators, domestic and international informed, if required by law, and where appropriate
    - Determine if there are there any additional regulatory reporting requirements
- Insurance:
    - What is the status of insurance claim documentation?
    - Coordinate claim with insurance broker and carrier for completeness and within terms of policies
    - Are there any outstanding issues?
- Information Technology:
    - What is the status of the technology infrastructure impacts and response/recovery efforts?
    - Was coordination of the response effort effective?
    - If disaster recovery plan was invoked, was the plan effective?
- Operational Controls:
    - Assess operations to determine necessary revisions to data collection, retention, storage, and processing policies and procedures
    - Assess need for additional employee training in data protection policies and processes
    - Review contract provisions with third parties that handle sensitive data and information
    - Review relevant website privacy notices and terms of service; update as needed;
    - Review relevant agreements with individuals. Determine if form agreements need to be updated.
- Business Issues (coordinate with executive leadership):
    - What is the potential short-term impact on TrueBlue revenue?
    - What is the potential long-term impact on TrueBlue revenue?
    - What is the expected loss of business as a result of the incident?
- Cyber Incident Management
    - What parameters are necessary for a declaration that the incident is complete?
    - Incident should not be declared complete until all notifications and investigations are completed, reported to the proper management teams and accepted as complete

Below is a chart that describes the various activities that each team may consider.

Technical Response Team(TRT)	Incident Response Team (IRT)	Incident Management Team (IMT)
• Track and assess the status of remediation efforts for all teams involved in incident remediation. • Ensure a final, comprehensive functions check and/or business continuity check has been done to ensure there are no irregularities in the remediated systems • Identify the root cause of the incident	• Review and integrate/apply any new technologies or procedures that were agreed upon throughout the Cyber Security Incident Response process • Ensure that all records about the status of the incidents and other pertaining information are maintained in a safe and secure way • Ensure that access to incident data should be properly restricted. Emails regarding the	• Retain outside Counsel, public relations, credit protection services, and technical experts, as needed • Review status of all insurance related to this event including Cyber Risk insurance, communicate with Risk and Legal to determine next steps required • Communicate with Litigation Support to discuss options • Provide credit monitoring for impacted Stakeholders, if appropriate

Technical Response Team(TRT)	Incident Response Team (IRT)	Incident Management Team (IMT)

• If third party caused the event, ensure appropriate containment measures are taken
• Inform IRT that the IT portion of event has concluded from a technical perspective
	incident, as well as documents should be encrypted.
	• If PII/PHI was exposed, begin to align compromised data with customer names and addresses for notification.
	• Document and communicate a long-term schedule for the team. Schedule recurring status meetings. The schedule should be 24/7. Support Personnel and SMEs not currently being used are on stand-by to ensure that their services are available.
	• If third party caused the incident coordinate with:
	  ○ Finance
	  ○ Human Resources
	  ○ Supply Chain
	  ○ Operations
	  ○ Communications
	• Make a determination that incident, investigations and notifications are complete and refer to IMT that event should be declared resolved/concluded
	• Complete transcription of all event logs
		• Contact Regulatory Agencies as required (laws vary by state.*)
		• If the incident occurred at a third-party location, determine if a legal contract exists. Work with the Legal and data owner/custodian to review contract terms and determine next course of action
		• Determine strategy for notification to Stakeholders
		• Determine role of Law Enforcement
		• Assess if declaration of resolution is appropriate and notifications and investigations are complete
		• Review all event logs and schedules
		• Schedule Post Incident Review and Lessons Learned meeting with teams

17.7 Learning

Description and high-level steps:

The lessons learned phase of the incident response process is critical for identifying areas where TrueBlue can improve its security posture and incident response capabilities. This phase should be completed no later than one (1) week after the end of the incident, while the incident is still fresh in the minds of the Incident Response Team.

The lessons learned process begins with a thorough investigation of the incident. This includes gathering evidence, interviewing involved personnel, and analyzing the incident response plan. Once the investigation is complete, the Incident Response Team will develop a report that identifies the following:

- ***Root cause of the incident:*** What factors contributed to the incident occurring?
- ***Areas of strength and weakness in the incident response plan:*** What worked well? What could have been improved?
- ***Recommendations for improvement:*** What changes can we make to our security posture and incident response plan to prevent similar incidents from happening in the future?

A report developed from the Lessons Learned meeting will be used to update incident response policies and procedures and used as justification for new controls.

All formal actions taken during the incident will be reviewed by the Incident Response Team. Any corrections and/or opportunities for improvement identified during this review should be incorporated into the documented plan. This process does not replace any outage analysis or corporate post-mortem activity that may be performed.

The Incident Administrator is responsible for creating a final record of communication and collected evidence from the incident.

- A Post Incident Review will include the following:
  - Network Monitoring
  - Encryption Monitoring
  - Risk Assessment Procedures
  - Incident Response Procedures
  - Communications
  - Breach Notification Procedures
  - Evidence Collection Procedures
  - Chain of Custody Procedure
  - Log Collection Procedure
  - Forensic Analysis Procedure
  - Malware Analysis Procedure
  - Log Analysis Procedure
  - Configuration Procedure
  - User Account Termination Procedures
  - User Access Procedures
  - Lessons Learned Procedures
  - Media /Public Relations follow up on Incident
  - Insurance Notification Procedures
  - IT Support Services Incident Procedures

Full Incident Response Team

• After business operations have returned to normal discuss "lessons learned." Topics of discussion should include the following:
  o What transpired and what was done to intervene?
  o Was there reasonable preparation to prevent the incident?
  o Did the "alert" occur promptly? If not, why?
  o Could additional tools have helped the alert and recovery processes?
  o Was the incident sufficiently contained?
  o Was communication adequate, or is there opportunity for improvement?
  o What practical difficulties were encountered?
• Continuous improvement of the plan. Review what went well, what did not go well, as part of following the plan, from a technical approach or from a communications aspect?
  o Stop Doing – what did not work?
  o Start doing – what new thing should we do?
  o Continue – what worked well and should not change?

17.8 Planning and Prevention

Description:

There are literally hundreds of detailed steps that can go into "Planning and Prevention" – everything from ensuring the complexity of a strong password to holding annual user security awareness training. For purposes of this document, these key steps are highlighted:

#	Task	Responsible Team(s)	Status
P-01	Ensure that anything that was uncovered during the Learning phase is incorporated into plans and technical controls, policies, procedures, etc.	IRT, IMT	
P-02	Rehearse Incident Response Plan at least annually	All Teams	
P-03	Review Security policies, standards and procedures and ensure that they are mapped to NIST, and that all relevant security standards are adhered.	IRT	
P-04	Review the plan annually and refer proposed changes to the Cyber Management Incident Response Team	All Teams	
P-05	Introduce changes to the plan: When things change, as a result of new process, procedures or technologies, or as a result of an incident where it is an improvement. Refer all proposed changes to the IMT	IRT	
P-06	Review opportunity for new tools. If new tools are acquired , train people on them.	IRT	
P-07	Update any existing training materials to reflect changes in the Cyber Incident Response Plan.	IRT	
P-08	Ensure manager and technical training on the Incident Response Plan annually.	IRT	

#	Task	Responsible Team(s)	Status
P-09	Periodic Incident Response Technology Assessment by a reputable security firm	IRT	
P-10	Periodic Compromise Assessment by a reputable security firm	IRT	
P-11	Review all insurance policies for coverage for known probable events and how the insurance policy portfolio mitigates those risks including Cyber Risk Insurance	VP Risk Legal CMIRT	
P-12	Ensure that all contracts and agreements between parties is clear in the definition of breach, use known and understood definitions, and are clear on what notifications are required and when they are required. Create a contract abstract with key provisions including cyber notification, indemnity etc.	Legal	
P-13	Maintain and verify applicable breach notifications for legal, regulatory and compliance.	Legal	
P-14	Review and update Cyber communication plans (internal and external) for proper notification and message mapping	ICT IMT	
P-15	All notification messages are written (to the point possible,) reviewed and approved by leadership and Legal, are ready to go in the event of an incident.	Legal ICT IMT	
P-16	All customer, supplier and other stakeholder distribution lists are up to date	Brand Presidents Supply Chain IMT	
P-17	Deliver end user security awareness training	IRT IMT	
P-18	Deliver First Responder training	IRT	
P-19	Ensure all security policies are up to date and are continually effectively communicated and training is provided, regarding data collection, application outputs, confidential data on servers, desktops, cloud-based application and mobile devices	IRT ICT Legal	

#	Task	Responsible Team(s)	Status
P-20	Inventory applications which are allowed on servers, desktops, laptops, cloud-based and mobile devices. Update 'whitelist' for these applications.	IRT	
P-21	Ensure all security procedures are up to date and are used in everyday practice	Technical Response Team	
P-22	Ensure the technical teams are place with the appropriate skill level to identify and respond to an incident – or have a third party skilled team on call	IRT	
P-23	Conduct periodic risk assessments of systems and processes – update policies and technology as a result if needed.	IRT	
P-24	Coordinate with Internal Audit for annual assessment of Cyber related controls and procedures	Internal Audit	
P-25	Create/Have/Document baselines of expected network, system and application activity	IRT Technical Response Team	
P-26	Update contacts for Law Enforcement	Legal VP Risk	
P-27	Update contacts for Outside Legal Counsel, forensic experts, crisis management and public relations	Legal IT Security ICT	
P-28	Conduct an inventory of sensitive data on servers, desktops, laptops, cloud-based applications and mobile devices	Technical Response Team IRT	
P-29	Ensure backups are being performed and verify the integrity of the backups periodically	Technical Response TeamIRT	
P-30	Create/Update Communication plan to include a Cyber document and detailed distribution of communications plan	ICT Brand Presidents	

#	Task	Responsible Team(s)	Status
		IMT	
P-31	As part of any planning process, ensure the proper information for users to know how to "Alert" the proper teams for when they come across an incident is available and trained.	Technical Response Team IRT IMT	

18. Incident Recording and Reporting

Cyber security incidents are a growing threat to organizations of all sizes. In order to effectively respond to these incidents, it is important to have a process in place for recording and reporting them. An incident report provides a detailed record of what happened, who was involved, and any injuries or damage that occurred. This information can be used to investigate the incident, identify the root cause, and take corrective action to prevent it from happening again.

All incident response forms can be found in Appendix A.

In addition to the incident response forms, TrueBlue will report all incidents to interested third parties. These third parties include:

- Information owners, such as business partners or clients who provide personal information.
- Third party organizations, clients, service providers or vendors that are connected to affected networks.
- Board of Directors, Board of Trustees or similar governance organizations who must be aware of significant or material threats to the organization.
    - Please be sure to check with the Legal and Compliance teams for the latest, and most accurate information of regulatory compliance and governance bodies.

SEC Form 8-K

Effective 9/05/2023, all SEC registrants are required to file a Form 8-K to disclose all "Material Cybersecurity Incidents" within four (4) business days from the date that an incident is considered material to the registrant. The SEC defines a cybersecurity incident as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

In addition, the final rule broadly defines "information systems" to encompass resources owned or used by the registrant (e.g., cloud-based or hosted systems) and will require issuers to consider incidents occurring both internally and within third-party service providers. A cybersecurity incident could occur accidentally or because of a deliberate attack.

19. Appendix A: Incident Response Forms

These forms should be completed using ink on paper.

Prepare your Incident Response Book by making several blank copies of these forms so that they are on hand during the incident response. Each form indicates the number of blank forms that should be kept in the Incident Response Book to ensure their availability when an incident is in progress.

Below is a list of the forms that can be found in TBI_Incident Response Plan_2023 - Ancilliary - Forms and Templates.docx, and the X indicates what phase they are either completed in, or used in.

Form	Triage	Investigation	Containment	Eradication	Recovery	Learning
Form A – OBSERVATIONS AND ACTIONS LOG	X	X	X	X	X	X
Form B – INVENTORY OF IMPACTED ASSETS	X	X	X	X	X	X
Form C –INCIDENT CLASSIFICATION	X	X				X
Form D – IMPACT ANALYSIS WORKSHEET		X				X
Form E – THIRD PARTIES CONTACTED	X	X	X	X	X	X
Form F – CHAIN OF CUSTODY FORM	X	X	X	X	X	X
Form G – ROOT CAUSE ANALYSIS FORM					X	X
Form H – INTERNAL INVESTIGATION REPORT					X	X
Form I – STATUS MEETING MINUTES	X	X	X	X	X	X
Form J – RESPONSE APPROACH	X	X	X	X		X

20. Appendix B: Updating the Incident Response Plan

The Incident Response Plan will be updated for a number of reasons, including:

1. A root cause finding at the end of an incident or event found that the Incident Response Plan needed to be improved,
2. Membership, roles, or responsibilities of the RT members have changed,
3. Management determined that the IRP needed to be changed to address new risks or responsibilities,
4. A cause for improving the plan was discovered during a test or walkthrough of the plan, or
   When the IRP is being updated:

   - The Roles and Responsibilities and RT membership must be updated and complete to include the **name** and **title** of each RT member and their RT **role**. All **contact information** for each team member must also be up-to-date.
   - All contact methods for reaching the RT members should be verified as up-to-date. *These hotlines must be communicated to all personnel if they are changed!*
   - The Authorities Contacts table must be updated.
   - Incident Response Experts are to be listed.
     a. An **Incident Response Expert** must be listed as stated above. Keep this contact information in both tables. When incidents occur, it is easy to overlook critical players. Reiterating the Incident Response Expert's name will reduce frustration as you are trying to locate first responders.
     b. **Security Vendor Websites**, including vendors that provide your Antivirus, log management and related security technologies very likely have incident contact numbers. Ensure that these numbers are up-to-date
     c. **Information Security Special Interest Groups** (SIGs) are informative when security vendors are not immediately helpful. Ensure that contact information for known Special Interest Groups such as first.org and isc.sans.org are available to help diagnose and respond to unexplained security phenomena.
     d. All third party Contact information including Law enforcement, Insurance Carrier/Broker, Third Party Cloud provider contacts, forensics, Outside Counsel, Crisis Management, Customers, Suppliers, **Credit Protection Agencies** should be listed and up to date. In the event that a data breach incident occurs, stakeholders and others may need to be contacted quickly.

During an incident, it is often critical to contact interested third parties to inform them of liabilities or impacts that they may incur due to an incident. Be sure to list possible third parties in the Interested Third Parties Contacts table for quick reference when an incident is under way.

Finally, be sure to update the version and date of the document at the footer of each page. Ensure that the current version is available to the RT only, and that all previous versions are no longer accessible to the team.

21. Appendix C: Glossary and Acronyms

ACL: Access Control List - A set of data associated with a file, directory, or other network resource that defines the perm ions that users, groups, processes, or devices have for accessing it. The list has an entry for each system user with access privileges.

Attack (noun) - An action conducted by an adversary, the attacker, on a potential victim. A set of events, which an observer believes to have information assurance consequences on some entity, the target of the attack.

Attack (verb)- To begin to act upon destructively, to begin to destroy, expose, alter, or disable.

Attacker - An adversary who conducts an attack on a victim (e.g., host). Contrast with intrudes.

Availability - The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

Breach - See intrusion

Chain of custody - Verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and times. For a proven chain of custody to occur, the evidence is accounted for at all times.

Computer Security Incident - Any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of such events are: intrusion of computer systems via the network (often referred to as "hacking"), the occurrence of computer viruses, probes for vulnerabilities via the network to a range of computer systems (often referred to as "scans") in the computer security arena, these events are often simply referred to as incidents.

Computer Security Incident Handling - By providing the basic set of services (triage, handling, and request), a team offers a defined constituency support for responding to computer security incidents. In addition to this basic set, an announcement service might also be offered.

IRT- An acronym for "computer security incident response team." This is a team

Providing services to a defined constituency.

Constituency- A specific group of people and/or organizations that have access to specific services offered by a IRT.

Confidentiality - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity)

DDoS: Distributed Denial-of-Service. A DDoS attack on TrueBlue means a flood of incoming packets from compromised systems are sent simultaneously. The goal of a DDoS attack is to overload the Company's system and shut it down, thereby resulting in denial of service to TrueBlue customers.

Event - An action directed at a target, which is intended to result in a change of state (status) of the target.

Exploit (verb) - To, in some way, take advantage of a vulnerability in a system in the pursuit or achievement of some objective. All vulnerability exploitations are attacks but not all attacks exploit vulnerabilities.

Exploit (noun) - Colloquially for exploit script: a script, program, mechanism, or other technique by which a vulnerability is used in the pursuit or achievement of some information assurance objective. It is common speech in this field to use the terms exploit and exploit script to refer to any mechanism, not just scripts that uses vulnerability.

IDS: Intrusion Detection System. A system used to monitor suspect activity either across network segments (Network IDS, NIDS) or on a specific computer (Host IDS, HIDS).

IP: Internet Protocol.

IPS: Intrusion Prevention System.

Impact - The negative effect of an attack on a victim system by an attacker. The use of this term occurs most frequently in incident analysis.

Incident - A collection of data representing one or more related attacks. Attacker, type of attack, objectives, sites, or timing, may relate attacks.

Incident handling/response - Actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event occurs; involves contingency planning and contingency response.

Information assurance - The sub field of information science that focuses on the conditions necessary to assure users of information systems and services that they can expect.

Integrity - For systems, the quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. For data, the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Intrusion - Actual illegal or undesired logical entry into an information system; the act of violating the security policy or legal protections that pertain to an information system. Intrusion seems to imply forced entry, while attack seems to only imply the application of force.

Intrusion detection system - A combination of hardware and software that monitors and collects system and network information and analyzes it to determine if an attack or an intrusion has occurred. Some ID systems can automatically respond to an intrusion.

Intrusion detection technologies - A broader term meaning a combination of ID systems, intrusion analysts, and other supporting tools. Used together, ID technologies can provide accurate indicators of whether or not an attack or intrusion has occurred.

Malware: Malware (short for "malicious software") is any program or file inserted into a system for a harmful purpose. Malware includes computer viruses, worms, Trojan horses, and spyware.

Monitoring - Observing a data stream for specified events to provide data for subsequent action or analysis.

Network Intrusion: Network intrusion is any malicious activity performed on a TrueBlue system (e.g., DDoS attacks, port scans, attempts to crack into computers by monitoring network traffic).

NIDS: Network Intrusion Detection System. An intrusion detection system that monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.

Preventive System: Any technical control in place to restrict access and/or reduce vulnerability to threats.

Phishing: Phishing involves the mass distribution of email messages that appear to have been sent from TrueBlue, a TrueBlue subsidiary, or a TrueBlue partner. These messages have return addresses, links, and visual branding (logos, etc.) that appear – to the untrained eye – to be identical to legitimate Company email communication. These fraudulent messages are designed to fool the recipients into divulging sensitive information (e.g., social security numbers, PINs, etc.).

Response - Actions taken to protect and restore the normal operating condition of computers and the information stored in them when an attack or intrusion occurs. Also referred to as incident response or intrusion response.

Security - The sub field of information science concerned with ensuring that information systems are imbued with the condition of being secure, as well as the means of establishing, testing, auditing, and otherwise maintaining that condition.

Social Engineering - Social engineering is the art and science of getting people to do something you want them to do that they might not do in the normal course of action. Instead of collecting information by technical means, intruders might also apply methods of social engineering such impersonating individuals on the telephone, or using other persuasive means to encourage someone to disclose information. Social engineering refers to any attempt to deceive someone into revealing confidential information about the Company, its customers, or employees. It also refers to tricking someone into breaking normal security procedures for the purpose of accessing TrueBlue information systems. The goal of social engineering is to commit fraud, network intrusion, industrial espionage, identity theft, or system or network disruption.

System - One or more interconnected physical machines (hosts) operating in cooperation with one another to meet a particular mission. Systems are generally, although not necessarily, contained within one site. Hosts may participate in multiple systems. Systems may be wholly contained within one host or distributed across multiple hosts.

Target (noun) - The object of an attack, especially host, computer, network, system, site, person, organization, nation, company, government, or other group.

Target (verb) - To use something or someone as a target. To plan or schedule something or someone to attain an objective. For many computer-based attacks, target selection and attack are tightly integrated and, perhaps, indistinguishable.

Threat: A potential cause of harm to the confidentiality, integrity, or availability of information or information systems.

Triage - The process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling.

Unauthorized Access: Unauthorized access is the act of gaining access without proper perm ion, from within or outside the Company, to any network, system, application, data, or other IT resource, with the intent to perform an action(s) that is deemed in violation of corporate policy.

Vulnerability - The existence of a software weakness, such as a design or implementation error, that can lead to an unexpected, undesirable event compromising the security of a system, network, application, or protocol.

Zero Day: Zero-day malware is a virus that is so new its definition is unknown and no signature has been established for it yet. Zero-day exploits may not be detected automatically by the Companys' anti-malware appliances. These viruses will come to the attention of IRT by different routes (e.g., intrusion detection appliances, internal router-based anomaly detectors, business lines). They will only be detected through careful analysis and must be resolved differently than other malware incidents.

END OF DOCUMENT