**1610: Introduction**

 **Model Content Revised Date: 11/26/2024**

Cyber incidents, like other types of disruptions, can have immediate and long-term impacts and enterprise-wide consequences. They can result from a variety of causes, both malicious and non-malicious, with impacts to hardware, infrastructure, applications, and data. Planning for cyber incidents, however, has significant differences from the other Business Continuity event/incident types that we plan for (Facility, Systems, and People).

Malicious cyber incidents involve malicious actors trying to compromise the availability, integrity, or confidentiality of computer systems, networks, and data. The specific cause of an incident may not be known while it is happening and my not be discovered until a forensic investigation is conducted over a period of days, weeks, or even months. These malicious incidents include (but are not limited to):

* **Denial of Service (DoS)**, where computer systems and networks are flooded with traffic in an effort to overload them and disrupt normal, legitimate activity.
* **Malware, including Ransomware, Spyware, Trojan-ware, Malvertising, and Worms**. These are commonly delivered by **Phishing**efforts through e-mail or Smishing via text messages tricking people to click a link that downloads malware or reveals login credentials.
* **Third-Party and Supply Chain Attacks**, where attackers infect trusted suppliers of applications and services and use them to gain access to your cyber assets.

Non-malicious cyber incidents can occur as a result of human error, structural failure or organization computer systems, infrastructure, applications, or facility or environmental controls, and natural disasters.

*Cyber Incident Response Life Cycle*



The purpose of this document is to identify the roles, responsibilities, actions, and resources used in the Cyber Incident Response process at [[CUname]] (Credit Union). It is designed to provide information and process guidance to support the knowledge and expertise of the Cyber Incident Response team and NOT to act as a step-by-step procedure manual.

Inside, you will find a high-level Cyber Incident Process Flowchart, Roles and Responsibilities for members of the Credit Union Cyber Incident Response team, key contact information, detailed guidance on critical portions of the cyber incident response process, and resources used to support cyber incident response activities at the Credit Union.

Please NOTE: The Preparation segment of the Cyber Incident Life Cycle is located in the *Appendix: Full Cyber Incident Life Cycle*, as it is done separately from the response activity segments.

[[CUname]] is the owner of this document, which is reviewed and updated following cyber exercises and actual cyber incidents to apply lessons learned towards the betterment and maturity of the Cyber Incident Response process. It is distributed to each member of the Cyber Incident Response team following each update.