**Nwachukwu Edumanichukwu**

**CYBR 445 - Advanced Incident Detection and Response  
Module 12 Lab – Measuring Cybersecurity IR Maturity**

In this 11th lab, you will fill complete the High-Level CREST CSIR Maturity Assessment Tool.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

Accessing the Lab

Download the CSIR Assessment Tool from here: <https://www.crest-approved.org/approved-services/cyber-security-incident-response-maturity-assessment/>

Additional instructions on filling out the CSIR Assessment Tool can be found here: <https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Maturity-assessment-tool_Info1.pdf>

If you still don’t feel confident in your ability to determine maturity levels, consider taking some take time to complete the Tutorials Point tutorial on CMMI here: <https://www.tutorialspoint.com/cmmi/index.htm>

Part I – Completing the CREST CSIR Maturity Assessment Tool

There is only one part to this lab. In some cases, you will directly receive instructions for filling out the appropriate fields. In other cases, you will have to make a subjective decision based on the description of the organization given. This will mostly relate to the maturity level of each assessed item. Reference the definitions for each maturity model below:

**Maturity Model Definitions:**

* **Foundational/Initial**
  + This maturity level is found in an unstable environment. The organization is highly reactive in putting out fires. Processes are ad hoc and the organization is relying on individual experience to keep things running. Processes are new and will not be documented. Processes are probably not repeatable, especially as the work is completed by different individuals.
* **Emerging/Established**
  + Includes all the requirements at the foundational level. Most processes follow a defined process that includes establishing requirements and processes that are planned, performed, measured, and controlled. Processes are followed and don’t break down during times of stress. Plans and processes are documented but documents are not necessarily mature. Work products are reviewed by stakeholders and objectives,

standards, and requirements are developed for processes.

* **Established/Business Enabling**
  + This includes all requirements of the foundational and emerging levels. Documentation is more mature at this level and includes a hierarchy of policies, procedures, standards, checklists, and guidelines. All processes are rigorously documented at each level and followed throughout the organization. Processes are repeatable no matter who is performing them or how long they have been at the organization if they meet a minimum qualification standard for their role.
* **Dynamic/Quantitatively Managed**
  + This includes all requirements of the foundational, emerging, and established levels. Key performance metrics are developed and tracked for all important processes and procedures. Stakeholders continually monitor the metrics associated with appropriate processes. Metrics are used to detect problems and the performance of processes is predictable.
* **Optimized/Optimized**
  + This includes all requirements of the foundational, emerging, established, and defined levels. Processes are continually improved based on the metrics analyzed at the previous levels. This level focuses on developing innovative improvements and improvements are quickly made. Agile processes may be established. While at the previous level, the primary concern is measuring processes and fixing things that are broken, improvement is the primary goal of this level.

1. Open the CSIR and click Enabling Editing when prompted at the top of the Excel Window.
2. Read the Introduction worksheet. Tabs are located at the bottom of the Excel window.
3. Read the Guidelines worksheet. Tabs are located at the bottom of the Excel window.
4. Fill out the following information on the Profile and Scope Worksheet:

**Scope of Assessment**

* Name of the area of assessment: Initial Assessment
* Business Unit: Cyber Fusion Center
* Organization: Bellevue Bank and Trust
* Sector: Retail Banking
* Scope of Assessment: Whole Organization
* Key Components: Security Operations Center, Incident Response, Threat Intelligence, Threat Hunting, Digital Forensics.

**Respondent Details**

* Date of assessment: today’s date
* Name of respondent: your name
* Role or position: Senior Cybersecurity Analyst
* Department: Cyber Fusion Center
* Organization: Bellevue Bank and Trust
* Type of Assessment: Internal
* Qualifications of Assessor: CREST
* Qualifications of Assessor: GCFA, GCIH, CCNA Cyber Ops

1. Fill out the following information on the Configuration worksheet:

**Phase 1 – Prepare**

* All target maturity levels should be optimized
* Steps 1, 2, 4, and 5 should have weightings of 2. The organization wants more of a focus on the preparation items that will most help in the response phase. Step 3 should have a weighting of 1.
* Evidence required should be: Policies, Standards, Procedures, Metrics, and Historical Evidence of Improvement.

**Phase 2 – Response**

* All target maturity levels should be optimized.
* Steps 1, 3, and 4 should have weightings of 3, Step 2 should be 2. There is a high focus on the response items that quickly identify and correct security incidents.
* Evidence required should be: Policies, Standards, Procedures, Metrics, and Historical Evidence of Improvement.

**Phase 3 – Follow Up**

* All target maturity levels should be optimized.
* Steps 1, 2, and 5 should have weightings of 3, Steps 3 and 4 should be 2. Step 6 should be 1. The organization wants more of a focus on the preparation items that will most help in the response phase.
* Evidence required should be: Policies, Standards, Procedures, Metrics, and Historical Evidence of Improvement.

1. Use the narratives below for each of the three phases to fill out the current level of maturity for each step under each phase. Provide your reasoning for your rated level of maturity and include a comment on the evidence available to support your reasoning.

**Phase 1 – Prepare**

Bellevue Bank and Trust has historically performed a criticality assessment annually for the past three years. There have been big problems with them in the past. First, there is not a good inventory of assets available and the inventory that does exist has holes. Assets are missing, not all hardware assets have a good inventory of the software installed on them, most assets don’t have business owners in the inventory databases and currently, contacting owners of an application or asset relies on tribal knowledge. Assets that are accurately recorded in the inventory database are not accurately mapped to a business application or business unit. There is a policy addressing accurate inventory of hardware and software, but it hasn’t been updated, reviewed, or followed well in the past. Bellevue Bank and Trust has just hired a new manager to stand up a technology asset management team to improve the inventory, but it may take up to the next year to complete the project and have an accurate and maintained inventory. This has caused problems with the criticality assessment because business applications and assets have not had correct criticality assigned during the assessment in the past or assets and applications have been missed. Standard metrics for the criticality assessment aren’t tracked or improved year over year. The bank does not have an in-house or contracted threat analyst team and threat feeds directly to the SOC or technology employees.

Metrics for threat feeds are not tracked and there have not been any tabletop exercises or threat assessments that use existing threat intelligence. It is mostly used for informing the vulnerability assessment team what to patch and for the SOC and IR team to look for indicators of compromise that match the threat feeds for high criticality intelligence. All employees receive annual phishing training, but no other cybersecurity training is given. No discussions about cybersecurity are held outside of senior executives and cybersecurity employees. The IT department does a good job of documenting security controls. They have implemented EDR, AV, Firewalls, IDS, mail security, MFA, and other security tools. Security tools are well documented, and documentation follows strict requirements. Each tool has corresponding policies, procedures, standards, and processes documented as well as architecture and project documentation. Employees that maintain each tool are sent to training for the tool, all security tools forward logs and alerts to the central Elastic Stack SIEM and use cases and alerts for each security tool are developed and documented. There are standard metrics for each tool that are reported each month. This is the result of a failed audit from the Federal Reserve five years ago, after which a lot of resources were provided to implement new and improve existing controls. Controls align to the CIS CSCs and NIST SP 800-53. No additional audits are done to assess the state of readiness, especially as it relates to known threats.

**Phase 2 – Respond**

Bellevue Bank and Trust has a mature security operations center, forensics, and incident response teams. Each team has a team charter. An in-depth IR plan has been developed. Policies, standards, and procedures exist for each team and function (IR, SOC, Forensics). BB&T also has an MSSP that sits in front of the internal SOC. They handle the first level of tickets and investigations and will escalate to the internal SOC anything that they can’t close themselves. SLAs have been established at all levels and metrics are reported monthly. The MTTD and MTTR for events and incidents have drastically improved over the last two years. For example, the last ransomware incident was contained within a few hours and only affected 3 servers and 2 workstations. Systems were restored within 24 hours! The biggest issue with the cyber fusion center (SOC, IR, Forensics) comes back to the lack of inventory. The only time SOC and IR are hampered is when they cannot find the owner of a system or when EDR tools are not installed on an endpoint or logs aren’t collected because no one knew about the system. This mainly affects the investigation aspect of response because events that take place on these systems are often manually reported, or it dramatically increases the investigation time. Improvements to detection, containment, remediation, and recovery are constantly tuned based on the metrics. Again, the one area that has resisted improvements is investigation and this is because of the poor tracking of bank hardware and digital assets.

**Phase 3 – Follow Up**

There are policies, procedures, and standards for incident follow-up. The SOC, IR, and Forensics Teams maintain an in-house capability for additional investigations such as malware analysis, IOC development, etc. Third-party vendors are also retained to perform additional investigations when needed, including providing additional IR, forensics, and malware analysis services. These services are utilized when internal services become overwhelmed or for events where there are financial or data losses. Detailed reports and metrics are available for Stakeholders and are quickly updated when new information is needed. Post-incident investigation reviews are rarely carried out currently due to the workload of current cybersecurity employees. All appropriate documentation exists to require them but due to the competitive environment for cybersecurity professionals, the bank has been unable to completely staff the cyber fusion center, so these are only carried out for the highest impact security incidents. No metrics for post-incident investigation reviews are carried out and no improvements are currently being made. As such, lessons learned and additional communication are only done for high-impact incidents for the same reason, even though they are required, and all documentation exists. The cyber fusion center does a great job of communicating with other technology teams and as such and IR reports are required by policy to have recommendations for improvement and remediation forwarded to appropriate teams in cases where there are security or technical deficiencies or vulnerabilities. Metrics for vulnerability management are tracked and the ability to reconfigure systems to reduce attack surface based on security events and incidents has greatly improved over time. Use cases, logging, and configuration are also improved in response to security incidents. All documentation exists for this feedback cycle. Trend analysis is done but metrics captured for trend analysis are basic and not often updated. This is again a limitation due to staffing issues.

1. When you have finished completing the document based on the narrative above, go to the results tab and make sure results for every phase and step exist and that the spider chart is correctly displayed. Save the spreadsheet and submit it to complete the assignment.