PwC and UGA Governance, Risk and Information Protection Case Study

Introduction

You have received a request from the Chief Information Security Officer (CISO) of Bulldog Home (BH) a leading smart home technology provider, to perform a maturity assessment against the NIST Cybersecurity Framework (CSF). With the recent high profile cyber breaches, they are concerned that Bulldog Home could be next. As a security professional, they expect you to evaluate the tools and controls currently in place and provide BH with recommendations to mitigate the issues that you identify.

Company Overview

Bulldog Home is an established and rapidly growing company that produces highly advanced smart thermostat devices. Bulldog Home's most prominent smart thermostat, TheTemp, was recognized last year by the Consumer Electronics Association (CEA), winning the CES Best of Innovations Award in the Eco-Design and Sustainable Technology category. Last year, revenue topped $1 Billion for the third time in a row.

There are two reasons for BH's success. First, they have invested heavily in R&D and their patented smart devices are considered some of the best in the market, primarily because of the proprietary composite materials they use and the sophisticated but simple technology leveraged within each product. The other reason for their success is their focus on customer interaction and satisfaction. BH uses social media aggressively to advertise, but also to connect directly with their customers even after a sale. This has resulted in a fiercely loyal customer base and BH estimates that close to 70% of their sales are from previous customers.

Bulldog Home is headquartered in Atlanta, Georgia. BH's primary manufacturing plant is in Mexico City where they control a wing in the manufacturing plant but share the rest of the facility with other companies. There is also a smaller facility in Atlanta that handles repairs and returns for any damaged products.

Instructions

Each team will perform a NIST CSF maturity assessment for Bulldog Home, each team will meet with Bulldog Home employees each week to discuss the security controls that are currently in place. At the end of the five week engagement, you will present your NIST Maturity Assessment Report to the client's leadership. You will use the steps outlined below to execute the engagement.

For purposes of this case study, student teams will be referred to as the "**Engagement Team**" and the PwC team members will be referred to as the "**Client**" or "**Client Team.**"

Step 1: Interview Client Teams

Before each week's Client call, review the material provided and the information discussed during class. Use the template in Appendix A to draft a list of questions and capture any additional information gathered during the meeting. You are to send your questions to your Client contact **at least 24 hours** before your meeting.

For each meeting, you should identify the following roles:

- **Engagement Leader** – Individual responsible for meeting kickoff, initial questions, and time keeping. There should be only one Engagement leader per week.
- **Note Taker** – The person who takes the "official" notes for the group. Other individuals should keep their own notes and work with the Note Taker to make sure that all important points are captured in the notes. The Note Taker is expected to send out the notes to all team members, including the client, as well as any action items.
- **Subject Matter Specialists (SMS)** – Any other team members who are not the Engagement Leader or Note Taker should act as Subject Matter Specialists. They are expected to actively participate in the discussions and ask questions they feel are relevant to the conversation.

Note: Each member of the team should rotate through each position throughout the course of the case study. If there are more team members than meetings, it is up to the team to spread out the assignments.

Step 2: Determine the Capability Maturity

Each week will have NIST categories associated with the meeting topics (see table below). After each client interview, discuss as a team how the controls reviewed during the client meeting impact the assigned NIST sub-category and determine the maturity level via the diagrams below. Compile all of the maturity ratings within the provided workbook.

Function	Category ID	Category Name	Category Description	Subcategory ID	Subcategory Description
	Govern	**GV.OC**	**Organizational Context**	The circumstances — mission, stakeholder expectations, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	**GV.OC-02**
	Govern	**GV.OC**	**Organizational Context**	The circumstances — mission, stakeholder expectations, and legal, regulatory, and	**GV.OC-03**

Govern				contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	
	Govern	**GV.PO**	**Policies, Processes, and Procedures**	Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced	**GV.PO-01**
	Govern	**GV.PO**	**Policies, Processes, and Procedures**	Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced	**GV.PO-02**
	Govern	**GV.RM**	**Risk Management Strategy**	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	**GV.RM-02**
	Govern	**GV.RM**	**Risk Management Strategy**	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	**GV.RM-03**
	Identify	**ID.IM**	**Improvement**	**ID.IM-02**	Security tests and exercises, including those done in coordination with suppliers and relevant third parties, are

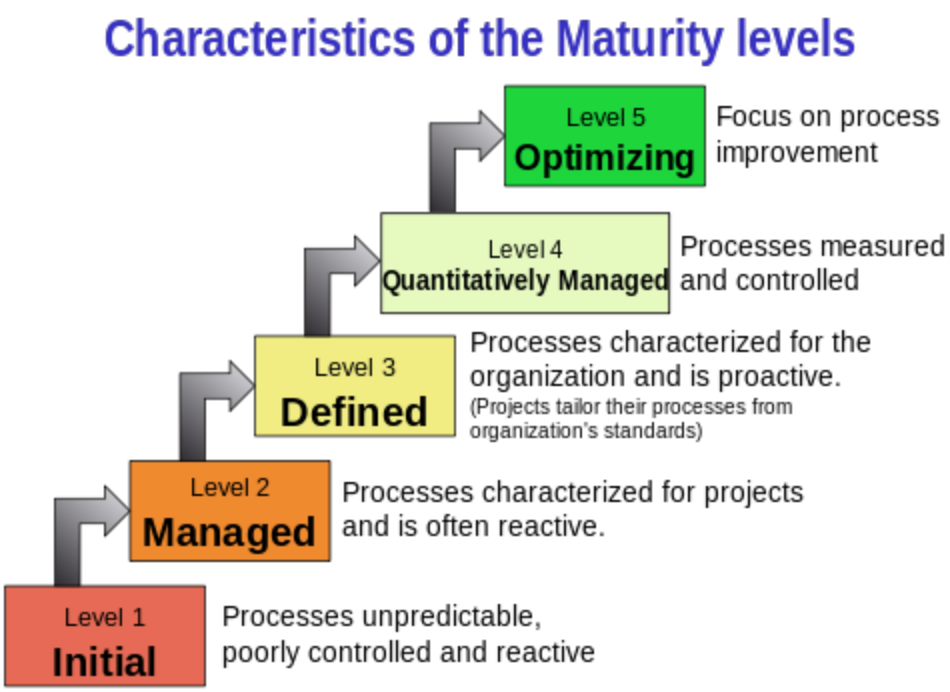
Identify					conducted to identify improvements
	Identify	**ID.IM**	**Improvement**	**ID.IM-03**	Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements
	Identify	**ID.RA**	**Risk Assessment**	**ID.RA-01**	Vulnerabilities in assets are identified, validated, and recorded
	Identify	**ID.RA**	**Risk Assessment**	**ID.RA-02**	Cyber threat intelligence is received from information sharing forums and sources
	Identify	**ID.RA**	**Risk Assessment**	**ID.RA-03**	Internal and external threats to the organization are identified and recorded
	Identify	**ID.RA**	**Risk Assessment**	**ID.RA-04**	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
	Identify	**ID.RA**	**Risk Assessment**	**ID.RA-05**	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization
	Identify	**ID.RA**	**Risk Assessment**	**ID.RA-06**	Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated

Protect	**Protect**	**PR.AA**	**Identity Management, Authentication, and Access Control**	**PR.AA-02**	Identities are proofed and bound to credentials based on the context of interactions
	Protect	**PR.AA**	**Identity Management, Authentication, and Access Control**	**PR.AA-03**	Users, services, and hardware are authenticated
	Protect	**PR.AA**	**Identity Management, Authentication, and Access Control**	**PR.AA-05**	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
	Protect	**PR.AT**	**Awareness and Training**	**PR.AT-01**	Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind
	Protect	**PR.AT**	**Awareness and Training**	**PR.AT-02**	Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind
	Protect	**PR.IR**	**Technology Infrastructure Resilience**	**PR.IR-01**	Networks and environments are protected from unauthorized logical access and usage

	Protect	**PR.IR**	**Technology Infrastructure Resilience**	**PR.IR-02**	The organization's technology assets are protected from environmental threats
	Protect	**PR.IR**	**Technology Infrastructure Resilience**	**PR.IR-03**	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations
	Protect	**PR.IR**	**Technology Infrastructure Resilience**	**PR.IR-04**	Adequate resource capacity to ensure availability is maintained
Detect	**Detect**	**DE.AE**	**Adverse Event Analysis**	**DE.AE-02**	Potentially adverse events are analyzed to better understand associated activities
	Detect	**DE.AE**	**Adverse Event Analysis**	**DE.AE-03**	Information is correlated from multiple sources
	Detect	**DE.AE**	**Adverse Event Analysis**	**DE.AE-04**	The estimated impact and scope of adverse events are determined
	Detect	**DE.AE**	**Adverse Event Analysis**	**DE.AE-06**	Information on adverse events is provided to authorized staff and tools
	Detect	**DE.AE**	**Adverse Event Analysis**	**DE.AE-07**	Cyber threat intelligence and other contextual information are integrated into the analysis
	Detect	**DE.AE**	**Adverse Event Analysis**	**DE.AE-08**	Incidents are declared when adverse events meet the defined incident criteria
	Detect	**DE.CM**	**Continuous Monitoring**	**DE.CM-01**	Networks and network services are monitored to find potentially adverse events
	Detect	**DE.CM**	**Continuous Monitoring**	**DE.CM-02**	The physical environment is monitored to find potentially adverse

					events
	Detect	**DE.CM**	**Continuous Monitoring**	**DE.CM-03**	Personnel activity and technology usage are monitored to find potentially adverse events
Respond	**Respond**	**RS.AN**	**Incident Analysis**	**RS.AN-03**	Analysis is performed to determine what has taken place during an incident and the root cause of the incident
	Respond	**RS.AN**	**Incident Analysis**	**RS.AN-08**	The incident's magnitude is estimated and validated
	Respond	**RS.MA**	**Incident Management**	**RS.MA-01**	The incident response plan is executed once an incident is declared in coordination with relevant third parties
	Respond	**RS.MA**	**Incident Management**	**RS.MA-02**	Incident reports are triaged and validated
	Respond	**RS.MA**	**Incident Management**	**RS.MA-03**	Incidents are categorized and prioritized
	Respond	**RS.MA**	**Incident Management**	**RS.MA-04**	Incidents are escalated or elevated as needed
	Respond	**RS.MI**	**Incident Mitigation**	**RS.MI-01**	Incidents are contained
	Respond	**RS.MI**	**Incident Mitigation**	**RS.MI-02**	Incidents are eradicated

Recover	**Recover**	**RC.CO**	**Incident Recovery Communication**	**RC.CO-03**	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
	Recover	**RC.CO**	**Incident Recovery Communication**	**RC.CO-04**	Public updates on incident recovery are properly shared using approved methods and messaging
	Recover	**RC.RP**	**Incident Recovery Plan Execution**	**RC.RP-02**	Recovery actions are determined, scoped, prioritized, and performed
	Recover	**RC.RP**	**Incident Recovery Plan Execution**	**RC.RP-04**	Critical mission functions and cybersecurity risk management are considered to establish post incident operational norms
	Recover	**RC.RP**	**Incident Recovery Plan Execution**	**RC.RP-06**	The criteria for determining the end of incident recovery are applied, and incident-related documentation is completed



Maturity levels of CMMI Institute: https://cmmiinstitute.com/

NIST Framework elements	Govern	Identify	Protect	Detect	Respond	Recover
Category data level	1-5 CMMI	1-5 CMMI	1-5 CMMI	1-5 CMMI	1-5 CMMI	1-5 CMMI
Subcategory data level	5. Optimizing 4.Quantitatively Managed 3. Defined 2. Managed 1. Initial	5. Optimizing 4.Quantitatively Managed 3. Defined 2. Managed 1. Initial	5. Optimizing 4.Quantitatively Managed 3. Defined 2. Managed 1. Initial	5. Optimizing 4.Quantitatively Managed 3. Defined 2. Managed 1. Initial	5. Optimizing 4.Quantitatively Managed 3. Defined 2. Managed 1. Initial	5. Optimizing 4.Quantitatively Managed 3. Defined 2. Managed 1. Initial

CMMI maturity-level definitions

5. Optimizing:	Process improvement incorporated to make process more effective as SOP
4. Quantitatively Managed:	Processes consistently managed and measured for performance consistency
3. Defined:	Processes consistently managed/performed
2. Managed:	Processes inconsistently managed/performed
1. Initial:	Processes lack sustainable, consistent management

Step 3: Develop Recommendations

After compiling the maturity rating for each NIST sub-category, develop recommendations for how Bulldog Home can increase maturity and include them in the provided workbook.

Step 4: Create Executive Presentation Deck

Use the template provided to create your presentation. Highlight the areas with the biggest weakness and develop thematic recommendations based on the areas with the lowest maturity. Rank the recommendation based on the order they should be implemented. Your report should remain tool agnostic since Bulldog Home plans to evaluate vendors and tools as part of a separate project.

You will be required to present your findings to the Bulldog Home security team. You should plan on taking no more than 15 minutes for your presentation and expect 5-10 minutes for questions from your Client.

Week 1: Introduction Week

This week will be used to familiarize the UGA teams with the PwC teams and discuss expectations for the case study. Key topics to discuss can include:

- NIST Workbook questions
- How to conduct phone interviews
- Key tips for conducting meetings
- Types of questions to ask during interviews
- Week-to-week expectations for the case
- Executive Presentation questions
- Roles and responsibilities

Week 2: User and Network Access

Client Team: Identify and Access Management (IAM) and Networking Team
NIST Category: Identity Management, Authentication, and Access Control, Awareness and Training
Background Information:

- Employees who switch roles within the organisation may maintain their previous access to systems, shared drives, and applications that they no longer require.
- When new employees join BH, access is based on the employee's job role and needs.
- Additional access required for an employee does require an approval from their manager, and is formally tracked through a centralized tool.
- If an employee is terminated, the manager has to submit an access removal request, which is processed within 2 business days.
- Most sales and customer support users have administrative access to systems with customer data and the customer facing applications to allow representatives to respond to customer needs as quickly as possible.
- Customers self register through Okta for the customer access portal. BH has limited capabilities to review a user's access and validate that the access given or removed is appropriate.
- BH relies on a pair of high availability firewalls at their perimeter to limit external traffic into the environment. The firewalls were recently upgraded to a best in class product, however, firewalls are only used to protect external traffic and are not used for internal connections
- An Intrusion Detection System (IDS) and/or an Intrusion Prevention System (IPS) solution is in place and has been updated over the last few years. However, the system is only utilized to monitor network traffic but does not perform any blocking. It will send a report daily to the security team showing the suspicious traffic it detected.
- Customer Reps can access the environment remotely using a VPN solution. The solution uses an RSA hard token for two factor authentication.
- The internal network is segmented from the DMZ

- Public web content is contained in a separate DMZ. There is a firewall restricting traffic from the DMZ and the internal network.
- BH has experienced minor issues over the past year due to unexpected high-volume traffic causing network failure.
- Public web content is contained in a separate DMZ. There is a firewall restricting traffic from the DMZ and the internal network.
- BH encrypts data at rest and encrypts data in transit between thermostats and network.

Key Terms:

- Identity Management Systems (IDM)
- Password Controls
- User Access Reviews
- Multi-factor Authentication
- Employee Onboarding and Termination
- Vendor Access Management
- High Availability Firewall
- DMZ
- Intrusion Detection/Intrusion Prevention System
- Network Segmentation
- TLS 1.2 Encryption (HTTPS Protocol)

Week 3: Security Operations

Client Team: Security Operations Center Team
NIST Categories: Incident Analysis, Incident Management, Improvement, and Adverse Event Analysis,
Background Information:

- BH has a security operations center that monitors and responds to security events within the environment
- The SOC is a team of two employees that also support other areas within BH's Security Department
- BH does have network security tooling and other detection tools that are configured across the environment
- BH collects and stores logs within a log repository. BH utilizes Splunk for monitoring.
- There are defined processes and documentation for responding to security events and incidents are tracked through an excel workbook.
- BH uses default windows native end-point capabilities to monitor devices but not all devices are supported within the data center since they use a mix of Windows and Linux servers
- Alert thresholds are in place to alert SOC analysts as they are defined within Splunk's native capabilities.
- Table top exercises are conducted for newly created detection processes and processes are reviewed yearly to ensure impact
- Security alerts are responded to as they come in and are not prioritized based on risk or impact. BH SOC analysts will investigate security events in the order in which they are discovered.
- Escalation processes are in place for responding to security incidents based on the business unit where points of contact are notified of an incident and are tasked with remediating the issue

Key Terms:

- Security Operations Center
- SIEM Tools
- End Point Detection Tools
- Incident Response Plans
- Security Alerting
- Logging and Monitoring

Week 4: Business Continuity and Disaster Recovery

Client Team: DR Team, BCP Coordinators
NIST Categories: Awareness & Training, Incident Recovery Plan Execution , Incident Recovery Communication , Incident Recovery Plan Execution
Background Information:

- BH has a formally documented Business Continuity and Disaster Recovery Plans.
- Each department designates a "Core Responder" who coordinates response activities in addition to their normal job role.
- Core Responders have to go through a Computer Based Training annually and are included in any drills. However, general system admins have not been included in any drills or training in the last year.
- In BH's policy for disaster recovery, we conduct an annual tabletop exercise to be performed by each department.
- In the past, drills have been focused on natural disasters (Tornados, Ice Storms, Pandemic)
- BH has annual testing and drills that have been tabletop simulation tests so as not to interrupt business operations.
- The business has determined that their Recovery Time Objective is eight (8) hours for normal operations and two (2) hours for payroll services.
- The business has determined that their Recovery Point Objective is five (5) days (i.e., they can lose up to five (5) days of data if their backup fails)
- BH has experienced a minor breach in the past but does not have a public relations department. The response to the public was handled by the CEO and Legal.
- BH does have a defined communication process for company executives when a business impacting outage or incident has occurred.

Key Terms:

- Types of drills (i.e. Parallel, Full Interruption, etc)
- Recovery Time Objective
- Recovery Point Objective
- Backup Schedules (Incremental, Differential, and Full)
- Disaster Recovery Plans
- Breach Management

Week 5: Governance, Risk and Compliance & Vulnerability Management

Client Team: GRC and Vulnerability Management Team
NIST Categories: Organizational Context, Policies, Processes and Procedures, Risk Management Strategy, Risk Assessment, Awareness and Training

Background Information:

- Security policy and standards have been created by BH but there is a defined process for making updates or adding new policies/standards.
- BH recently bought Archer to manage and track risks and findings, and implementation of the tool is still underway.
- BH is in scope for PCI compliance but historically have been too small of a company to be impacted and do not have clear delineation of security requirements for PCI compliance. However, this year BH is prioritizing compliance requirements and will undergo an audit.
- BH does have customers across the globe but does not have a defined Privacy program.
- Risk assessments are performed to determine business impact analysis for critical applications and systems that are in compliance scope or access customer personally identifiable information (PII), but are not done for all applications across the enterprise.

- BH does not have an enterprise wide asset inventory that is regularly updated.
- Risks that are identified by the Security team are logged into Archer, but there is a defined process for ranking the risk or determining the impact before being added to Archer.
- Identified vulnerabilities are assigned remediation owners and remediation SLAs, but there is no validation process to confirm that the vulnerabilities have been remediated.
- All employees are required to take the training on an annual basis. Training is performed via computer based training platform and must get a passing score to complete.
- BH does not have centralized third party vendor engagement and relationships.
- BH's third party manufacturer is asked to adhere to the security policies and standards set by BH, but security does not perform any periodic due diligence on their compliance with BH security policies.
- Roles and responsibilities for the security are documented, but that process is not formalized for other business units within BH.
- Business critical applications and systems follow a change management process, but it is not enforced across the organization. Additionally, there is no requirement for security testing to be conducted to confirm changes are not introducing new vulnerabilities into the production environment.

Key Terms:

- GRC Tools
- PCI Compliance
- Privacy Compliance
- Business Impact Assessments
- Change Management
- Security Testing
- Personally Identifiable Information (PII)
- Risk Ranking

Week 6: Security Team Review

Client Team: BH Security Team

Background Information:

Presenting draft NIST workbook findings and presentation to the BH Security team prior to presenting to the BH Senior Executives.