VESTEL R&D

INCIDENT RESPONSE PLAN

Date	**: 21/05/2019**
Version	**: V 0.1**
Unit	**:** VESTEL Electronics R&D, Manisa

ZORLU 50.yıl

Document History

Version	Date	Document Revision and Review History	Status	Prepared by	Approved by
V0.1	21/05/19	First creation	Draft	Oguzhan YAVUZ	

INDEX

EXECUTIVE SUMMARY

To maintain the trust of our customers, end-users and partners, and meet regulatory requirements, it is essential that we do everything we can protect confidential information and IoT solutions / systems in the face of a cyber-attack. The more we are prepared to respond to a potential cyber-attack, the faster we can eradicate any threat and reduce the impact on our business.

The goal of this incident response plan is to prepare Vestel Electronics to quickly and effectively contain a cyber-threat and risk for IoT solutions / systems. To this effect, actions outlined in the plan pay special attention to protecting accounts, credentials, sensitive data that use or transfer in IoT solutions such as databases, mobile applications, cloud backend, and IoT devices such as smart TVs, smart white goods and ICT products

Effective incident response involves every part of our R&D organization, including IoT R&D Group, TV software R&D Group, IoT Design Verification Group, legal, technical support, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be updated at least annually to reflect our changing organization, new technologies and new compliance requirements that inform our cyber security strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

1. ROLES, RESPONSIBILITIES & CONTACT

ROLE	RESPONSIBILITY	CONTACT DETAILS
INFORMATION SECURITY		
IoT Security Team Lead OR IoT Security Architect	Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan. Authorizes when and how incident details are reported. Main point of contact for executive team.	Ali Gürhan Gür gurhan.gur@vestel.com.tr
IoT security architect / Cloud architect / embedded system architect / mobile application architect / software test architect	Technical lead that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber-incident. Maintains incident response plan, documentation, and catalogue of incidents. Responsible for identifying, confirming and evaluating extent of incidents. Conducts random security checks to ensure readiness to respond to a cyber-attack.	Oguzhan Yavuz oguzhan.yavuz@vestel.com.tr
IoT Security Team / Cloud Development Team	Responsible for self-risk assessment, developing of security mechanism for providing security of IoT Solutions Discovers, audits, and reports on all IoT solutions. Monitors the traffic of IoT solutions and checks for indicators of compromise, such as excessive logins, or other unusual behavior. Manages security controls to limit progression of a cyber-attack across third-party systems and organizations. Informs incident response team of potential attacks, validates and reports on the extent of attacks.	Sena Yakut sena.yakut@vestel.com.tr
Project Management Office	Manages access to systems and applications for internal staff and partners. Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyber-attack.	Gökhan Çabuk gokhan.cabuk@vestel.com.tr
COMPLIANCE		

Legal Counsel	Confirms requirements for informing employees, customers, and the public about cyber-breaches. Responsible for checking in with local law enforcement.	Arda Aktan arda.aktan@zorlu.com
Audit & Compliance	Communicates with regulatory bodies, following mandated reporting requirements.	Arda Aktan arda.aktan@zorlu.com
COMMUNICATIONS		
Public Relations Lead	Communicates externally with customers, partners and the media. Coordinates all communications and request for interviews with internal subject matter experts and security team. Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	Şahika Özcan Ortaç sahika.ortac@zorlu.com
Web & Social Media Lead	Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users. Sets up monitoring across social media channels to ensure we receive any feedback or questions sent by customers through social media.	Şahika Özcan Ortaç sahika.ortac@zorlu.com
Technical Support Lead	Provides security bulletins and technical guidance to external users in case of a breach.	Emir Bacak emir.bacak@vestel.com.tr

2. THREAT CLASSIFICATION

The “CIA Triad” (Confidentiality, Integrity, and Availability) is a framework for incident classification that helps to prioritize the level of incident response required for a cyber-attack. CIA is as follows:

1. **Confidentiality** – Incidents involving unauthorized access to IoT solutions / systems, including account compromise, sensitive data breaches, manipulating of users. The more confidential the data or more important the systems are to the business, the higher the potential impact.

2. **Integrity** – Incidents involving data poisoning such as to corrupt or modify data. The more sensitive the data, the higher the potential impact.

3. **Availability** – Incidents that impact availability or proper functioning of services, such as Distributed Denial of Service (DDoS), including use of user accounts to make unauthorized changes. The more critical the services to the business, the higher the potential impact.

When ranking the level of risk to the organization and the type of incident response required, we take into account, credentials on IoT devices and sensitive data which are compromised. When end-user accounts are involved in the breach, the level of risk increases exponentially as does the response required.

SAMPLE CYBER INCIDENT	CIA CATEGORY	DATA BREACH	BUSINESS IMPACT	RISK LEVEL
Physical attacks: This sort of attack tampers with hardware components and accesses the credentials and limited sensitive personal data.	C	Yes	High	Low
Unauthorized discovery and mapping of services, or vulnerabilities on IoT devices by using of scanning network ports, packet sniffers, traffic analysis, and sending queries about IP address information	C	No	Medium	Low
Denial-of-service (DoS) or Distributed DoS	A	No	Medium	Medium
Unauthorized persons gain access to networks or devices to which they have no right to access. Remote access	C, I	No	High	Low
Privacy violation	C, I	Yes	High	Low
Cyber-crimes: IoT devices are used to exploit users and data for materialistic gain, such as intellectual property theft, identity theft, brand theft, and fraud	C, I, A	Yes	High	Low
A developer or an employ shares critical information with an unauthorized third party.	C	No	High	Low

3. COMPLIANCE AND LEGAL OBLIGATIONS

PCI DSS

PCI DSS provides organizations that accept, store or transmit credit card data with guidelines for privilege management and a framework to protect cardholder data.

- **Reporting requirements –** PCI DSS requirement 12.10 requires entities have an incident response plan and alert effected parties immediately. You may want to set up an arrangement with an independent Payment Card Industry Forensic Investigator (PFI) to call if you need outside expertise.
- **Learn more –** https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf

FISMA/NIST

The National Institute of Standards and Technology (NIST) outlines steps federal agencies and government contractors must take to comply with privilege management in FISMA in NIST SP 800-53.

- **Reporting requirements –** US-CERT has established a standard set of data elements that must be included in any incident report.
- **Learn more –** https://www.us-cert.gov/incident-notification-guidelines-2015

EU GDPR

Any organization dealing with EU citizens' Personally Identifiable Information is obligated to meet standards for effective data protection, adequate security measures, and privacy by design to comply with EU GDPR.

- **Reporting requirements –** Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals." This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.
- **Learn more –** https://www.eugdpr.org/key-changes.html

EU Cyber-Security Act.

The EU Cyber-security Act. introduces an EU-wide cyber-security certification framework for ICT products, services and processes. Companies doing business in the EU will be obligated to certify their ICT products, processes and services.

- **Reporting requirements–** Under the EU Cyber-security Act., the end-user should have access to information regarding the reference number of the certification scheme, the assurance level, the description of the cyber-security risks associated with the ICT product, ICT service or ICT process, In addition, the end-user should be informed of the cyber-security support policy which is that the end user can expect to receive cyber-security updates or patches, and there is a contact information of a single point of contact to report and receive support in the case of cyber-attacks.
- **Learn more –** https://eur-lex.europa.eu/eli/reg/2019/881/oj

TR KVKK

Any organization dealing with TR citizens' Personally Identifiable Information is obligated to meet standards for effective data protection, adequate security measures, and privacy by design to comply with TR KVKK.

- **Reporting requirements –** Under the KVKK, breach notification will become mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals." This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.
- **Learn more –** http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

UK Cyber Essentials

Contractors in the UK that handle sensitive or personal information must receive Cyber Essentials Certification to demonstrate understanding and enforcement of privilege management.

- **Reporting requirements –** UK Cyber Essentials uses external auditors to confirm compliance with the security framework and award certificates.
- **Learn more –** https://www.cyberessentials.ncsc.gov.uk/

4. INCIDENT RESPONSE STEPS

The incident process consists of six steps: preparation, detection, containment, investigation, remediation and recovery (NIST SP 800-61: Computer Security Incident Handling Guide). Vestel Electronics's incident response process steps are documented in specific procedures it maintains. This plan is the primary guide to the preparation phase from a governance perspective; local guidelines and procedures will allow the IoT R&D group to be ready to respond to any incident.

Preparation

Preparation includes those activities that enable IoT R&D group to respond to an incident: policies, tools, procedures, effective governance and communication plans to our customers and end-users. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage.

All public communications for an incident or incident response to the customers, end-user and external parties are made in consultation with Vestel customer service and legal office. Private communications with other affected or interested parties contain the minimum information necessary. The minimum information necessary to share for a particular incident is determined by IoT security team.

Detection

Detection is the discovery of the security event with

- Self-assessment of security risks on IoT solutions
- External risk assessment or external penetration testing
- Reported by outside people or parties about a suspected incident.

This phase includes the declaration and initial classification of the incident according to threat classification.

Containment

In this step, the affected sub-systems of IoT solutions are identified, isolated or otherwise mitigated, and affected customers, end-user and third parties are notified and investigative status established. Also this step consists of sub-procedures for evidence handling and communication.

Investigation

In this step, IoT security team determines priority, scope, and root cause of the security risk. After determining of security risks, first solution is proposed to other teams of IoT R&D Group.

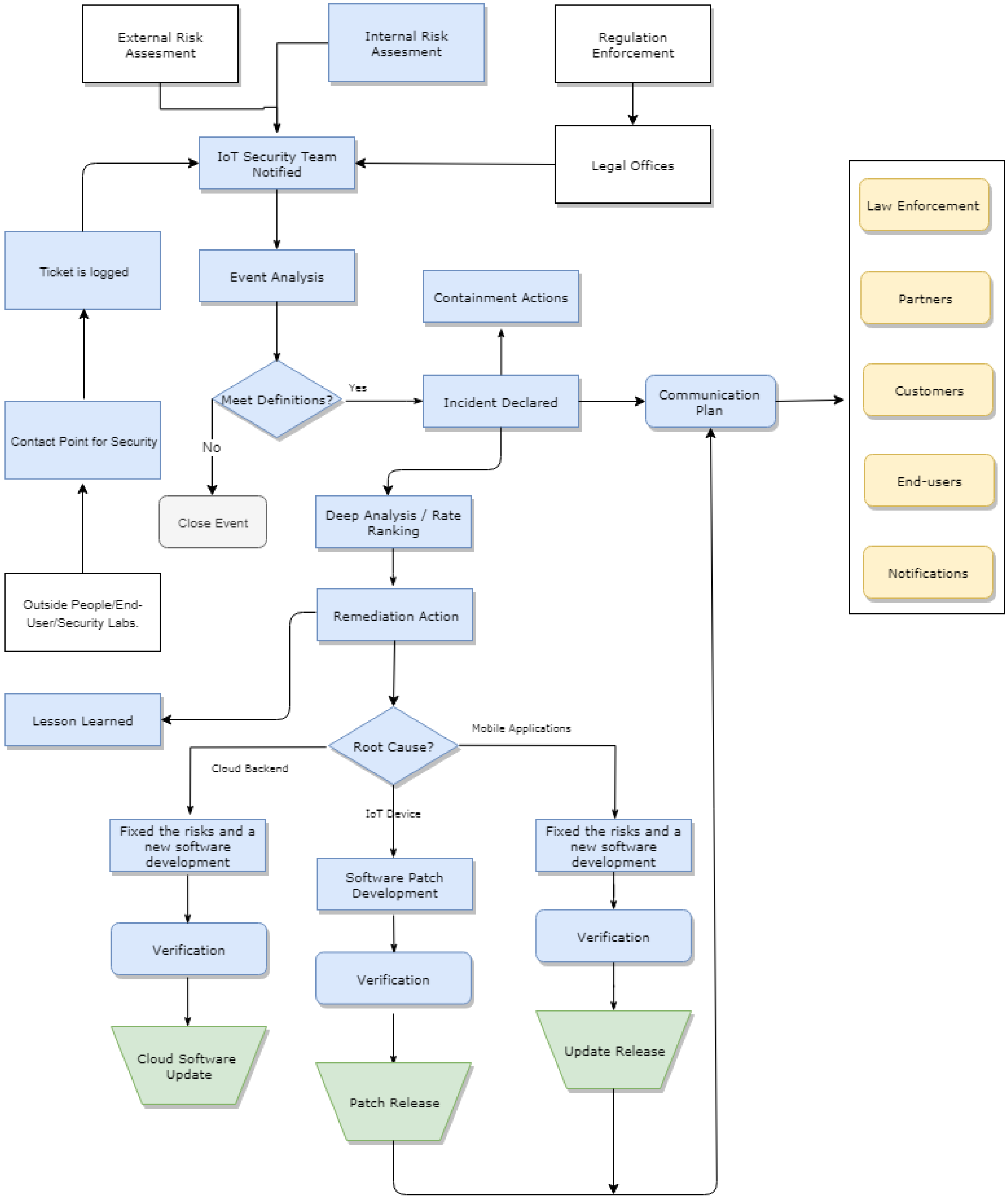
Remediation

In this step, the software patch is designed and developed to solve security risk and incident, and test solution that fixes threat. All reports and analysis will be completed at this step as it may impact the remediation and interpretation of the incident.

Recovery

In this step, if root cause of security incident is determined on IoT devices or mobile applications, a software patch that is verified for fixing of threat is prepared according to Vestel software update strategy. After patch is developed, all customers and end-users are informed by a public web-page or Vestel customer service team to implement the software patch on the IoT devices. In case of root cause is determined on Cloud backend, new software patch will be implemented. Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of “lessons learned” into future response activities and training.

5. INCIDENT RESPONSE PLAN PROCESS


External Risk Assesment
Internal Risk Assesment
Regulation Enforcement
IoT Security Team Notified
Legal Offices
Ticket is logged
Event Analysis
Containment Actions
Law Enforcement
Partners
Meet Definitions?
Yes
Incident Declared
Communication Plan
Customers
Contact Point for Security
No
Close Event
Deep Analysis / Rate Ranking
End-users
Notifications
Outside People/End-User/Security Labs.
Remediation Action
Lesson Learned
Root Cause?
Mobile Applications
Cloud Backend
IoT Device
Fixed the risks and a new software development
Software Patch Development
Fixed the risks and a new software development
Verification
Verification
Verification
Cloud Software Update
Patch Release
Update Release