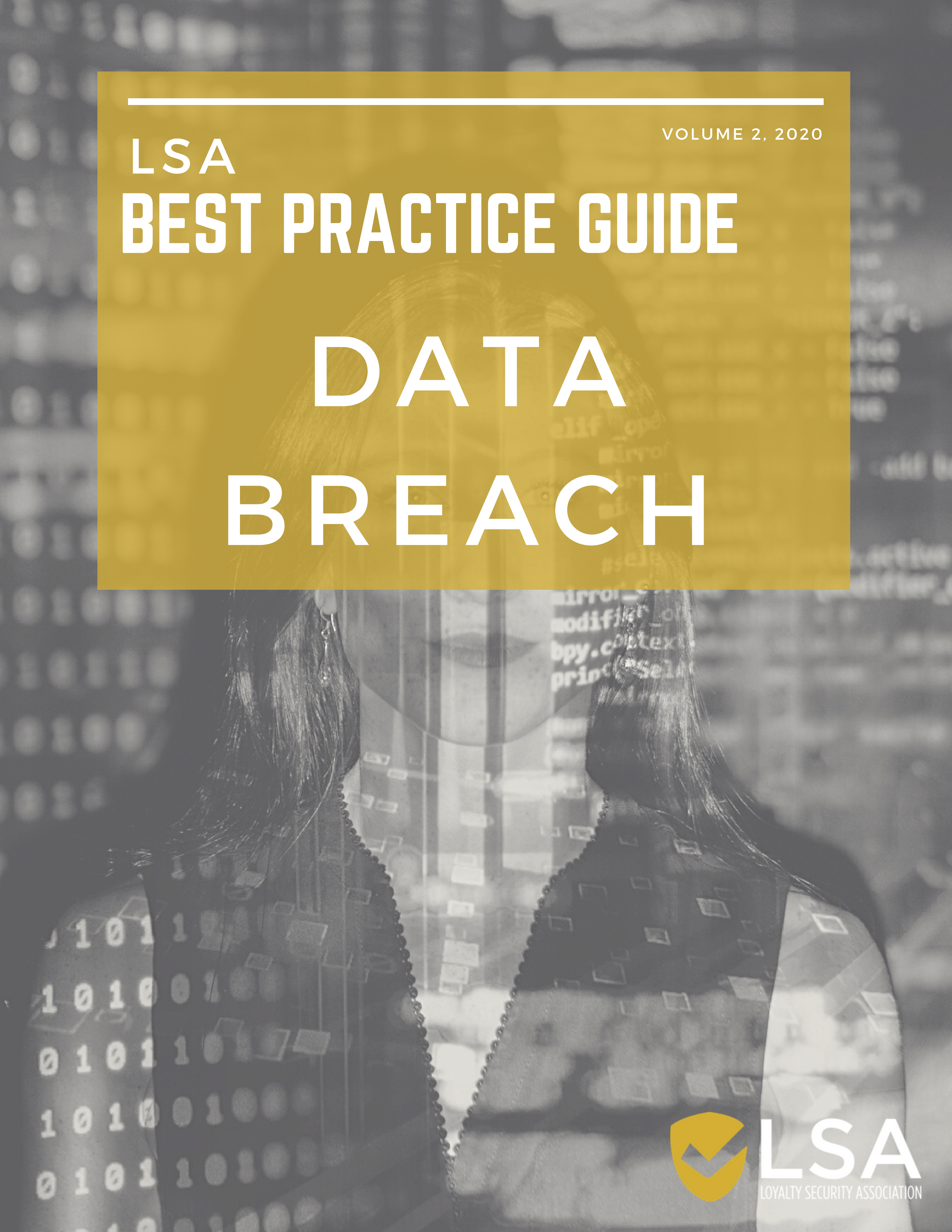


VOLUME 2, 2020

LSA

BEST PRACTICE GUIDE

DATA BREACH

LSA

LOYALTY SECURITY ASSOCIATION

TABLE OF CONTENTS

INTRODUCTION

When we founded the Loyalty Security Association, as the LFPA in 2016, it was in answer to a need in the Loyalty Industry. A need for information, advice, and help combatting Loyalty Fraud.

Loyalty and Payment Fraud hurt merchants of all types. The card payment industry realized long ago that they were fighting a common enemy and joined forces to develop and introduce tools and solutions to make card transactions more secure.

This led to a change in how fraudsters behaved, they now focused more on Loyalty; a field where the opportunities for a significant return on limited effort were wide open.

After all, the Loyalty Programs are on their own – there is no overriding body that defends their interest. No industry standard, yet, in defining the types of fraud, no set procedures or rules to live by, which leads to a struggle in limiting loyalty fraud losses.

The LSA offers a platform for Loyalty Programs to meet with their counterparts to discuss ways to reduce fraud, find providers with solutions, and start setting standards whilst sharing Best Practices.

Our event participants have requested us to develop a Best Practice Guide, and we are doing so with the help of industry experts. They will contribute their know-how in specific areas, with examples and guidelines, tips and advice.

We are publishing these chapters, rolling them out one-by-one for now, and bundling them in the future. It is the LSA's hope that you will not only enjoy reading these chapters, but most of all, find some useful information in them to take away and implement.

If you would like to contribute to our Guide or have a topic you would like to see included, let us know, we are in this together after all.

Maeder

PETER MAEDER
CO-FOUNDER, SECRETARY

Data Breach

What is a data breach?

A data breach occurs when a cybercriminal successfully infiltrates a data source and extracts sensitive information. This can be done physically by accessing a computer or network to steal local files or by bypassing network security remotely. The latter is often the method used to target companies.

IN THIS VOLUME

- Anatomy of a Data Breach
- Type of Attacks
- Controls to Reduce Risk
- Incident Management

Why are Loyalty Programs & Platforms a target?

Part of the business model for Loyalty programs is collecting and working with **Personally Identifiable Information (PII).** It is hard to put a value on PII as a lot depends on what data is involved, but traditionally you could expect that usable PII (name, postal address, personal email, phone number, date of birth, etc.) to reach around $8 per record.

Loyalty Specific Data (points & miles): With the modern offerings of competitive loyalty reward platforms including goods and services (including free nights, flights or upgrades) means the attributed value of points can be a **viable target** for attackers. These values, once taken, can be illegally redeemed against these goods or services, or sold, by the attacker. Items then have a resale value and make the proceeds of crime difficult to trace.

WHAT ARE THE CONSEQUENCES OF A DATA BREACH FOR LOYALTY PLATFORMS?

There are two main consequences to a Data Breach.

The first is financial, an organization will lose money; be it through having their accounts stolen or through fines imposed by financial institutions and regulatory organizations (e.g. The European Commission with the GDPR).

The other is the reputation damage, as customers will likely think twice before joining a Loyalty platform or program that has been breached in the past.

ANATOMY OF A DATA BREACH

Researching the Target
A data breach generally begins with the attackers researching the target organization in great detail to understand the operations. The attackers might look at job listings to find out what specific hardware and software the business uses. They might check financial filings and court records to learn how much the target spends on cybersecurity. Additionally, hackers may identify the target's business partners, because compromising them first might provide an entry point into the target's systems.

ANATOMY OF A DATA BREACH - CONTINUED

Scanning for Vulnerabilities
Attackers will scan the target's systems for vulnerabilities. Typically, they use software utilities that scan the target exposed services. Attackers will also attempt to enumerate everything on the target network; for example, systems and user accounts as these may provide a point of entry. Attackers will use tools that seek out known vulnerabilities, or perhaps check to see if the system has a relatively unknown weakness.

Exploiting Vulnerabilities
After identifying system vulnerabilities (assigned to an open port), the attackers will run exploit code (malware, viruses) that takes advantage of the weaknesses.

IT IS BEST PRACTICE TO CLOSE ANY PORTS THAT ARE NOT ASSOCIATED WITH A KNOWN LEGITIMATE SERVICE.

ANATOMY OF A DATA BREACH - CONTINUED

Delivering Payload
Now that the hackers have exploited the network, their next step is to deliver the payload. They might do so by uploading malware, hijacking servers, or taking over internal user accounts. By this stage, the hackers have intruded into their target's system, and are making sure they can access the valuable data they are seeking.

Extracting Data
Finally, hackers will download the data they were seeking, whether that's loyalty points/miles, credit card information, medical records, intellectual property, or something else. Good network security monitoring can pick up on this unusual traffic—but with strong cyber defenses, such as SOCVue, hackers won't be able to get this far.

Organizations that take a proactive security stance, including discovering and fixing weaknesses before hackers can find them, will be far better protected against a data breach like this. **The average time from a company getting hacked and finding it out is 24 weeks (roughly 6 months) meaning a criminal could be harvesting card data for during this time.**

TYPES OF ATTACKS

External Attacks

This term is usually meant to cover attacks emanating over the Internet and pointed towards external facing systems. Examples of Internet facing systems are websites, customer portals, VPN access points, and could include the primary and even redundant back-up systems to those sites.

The attacker could be anyone, a state sponsored actor, professional criminal, a bored university student or even a competitor. Protecting yourself from the more sophisticated attackers, such as state sponsored actors, is near impossible; however, as you move down the capabilities, customers expect organisations to be more able to deal with attacks.

Internal Attacks

Internal attacks usually combine a physical and logical element and are completed by or through personnel within the organization. The attacker is physically accessing a system, sometimes with the valid user rights they have been given to perform their role, and then making logical changes in systems to extract the information they wish to steal (such as PII, credentials, colleague SecureID).

Internal attacks often require less sophistication as they can bypass a number of security controls due to the trusted nature from where system requests originate from.

Controls to reduce the risk

Typical controls include a **mixture of people, processes, and technology**. In this section we will explore controls across all three areas. This is not intended to be a complete list of controls, but the controls identified will aid in bolstering the defenses of most organizations.

> *"A POORLY MANAGED INCIDENT CAN SEVERELY IMPACT REPUTATION AND TRUST WITH CUSTOMERS; HOWEVER, A WELL-MANAGED INCIDENT WITH CLEAR COMMUNICATION STRATEGIES CAN BE RECOVERABLE."*

Security Awareness Training

In any security control environment having a workforce that is cybersecurity aware is a key success factor. Aware staff can help spot and prevent security issues within the environment, so training staff and having appropriate training for different levels/types of staff is paramount.

Having a generic annual security awareness program will tick compliance type boxes, but it will not develop or evolve to a security aware culture. In this context staff with responsibility for security incident response should be trained and tested on the responses relating to a data breach. A poorly managed incident can severely impact reputation and trust with customers; however, an incident that was well-managed with clear communication strategies can be recoverable.

Controls to reduce the risk - continued

Security Testing
There are a number of methods an organization can employ to complete security testing; the best approach is to combine a number of these methods to gain a better understanding of external and internal exposures. So, in this section we will discuss the methods of security testing.

Vulnerability Scanning
A process to use tools to scan systems to identify security issues or misconfigurations. The approach to vulnerability scanning should focus on scanning internally and externally.

WebScan
WebScan is a free automated scanning tool that analyses websites for specific security vulnerabilities and produces a risk score.

It performs a passive scan of the publicly available information on the website, checking for Malware, Framework vulnerabilities, missing patches, and SSL certificate to ensure it is valid and using the latest security protocols. WebScan is not a full external vulnerability scan and at no point tries to exploit vulnerabilities.

This is a great step to know how vulnerable your loyalty website is.

Foregenix offers free scans for
your transactional or loyalty
website at foregenix.com/webscan.

Controls to reduce the risk - continued

Penetration Testing

Penetration testing is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. Penetration testing provides an organization an understanding of their exposure based on the scenarios explored. Testing can be performed internally or externally, depending on the assurance that is sought from the engagement. Organizations should look to document a strategy for penetration testing in order to get organizational support. For loyalty platform owners within an organization it should be ensured that loyalty is included in the testing activities. Organizations can look to the following in order to explore and document a strategy.

Security Monitoring

Traditionally organizations choose to deploy security incident and event monitoring (SIEM) tools to identify issues and raise these for review as required for PCI DSS certification. These tools are being replaced by proactive incident response (PIR) technologies which monitor organizations in real time, in order to minimize the breach window (time between infiltration and detection). These tools can be used to greatly reduce liabilities especially in relation to data breach scenarios.

Controls to reduce the risk - continued

Authentication Management
One area for all organizations to focus and improve is around authentication management. The use of multifactor authentication for users, especially those with privileged accounts or access to large amounts of data or to sensitive information can greatly reduce the exposure to risk of data breach. Multi-factor authentication, when implemented correctly, requires that attackers have credentials as well as another factor to access systems.

Controls to reduce the risk - continued

Audit and Third Party Assessments
External audit and assessment by organizations that specialize in Cyber Security can really help focus and measure the security maturity within an organization against defined external guidance or standards. Understanding the alignment to external best practices can help focus resources and provide assurance that risks are mitigated in line with organizational accepted risk levels or profiles.

Third Party Management
When organizations employ the services of third parties it is often assumed that security is implicit within the contracted services. Regulations like the GDPR make that responsibility sit with the data controller, so it is important that contracted services include security requirements, but also clauses to notify in the event of data breach and establish liabilities for each party.

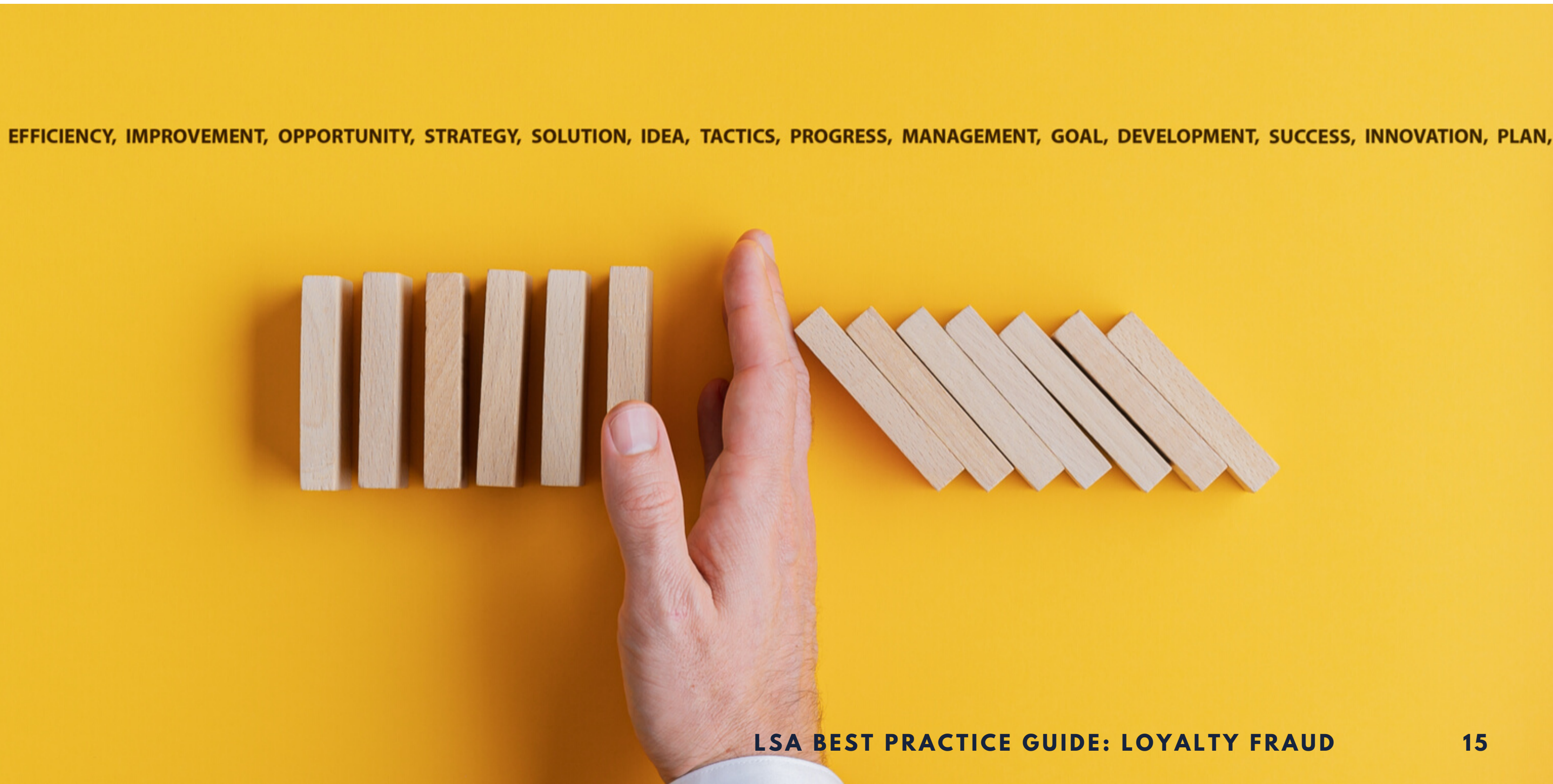
For third parties providing services to loyalty platforms the following should be included:

- Contract which defines legal obligations and liabilities for data breaches
- Responsibilities matrix for implementing security controls
- Demonstration of applicable certifications or standards implementation.

INCIDENT MANAGEMENT PLANNING AND TESTING

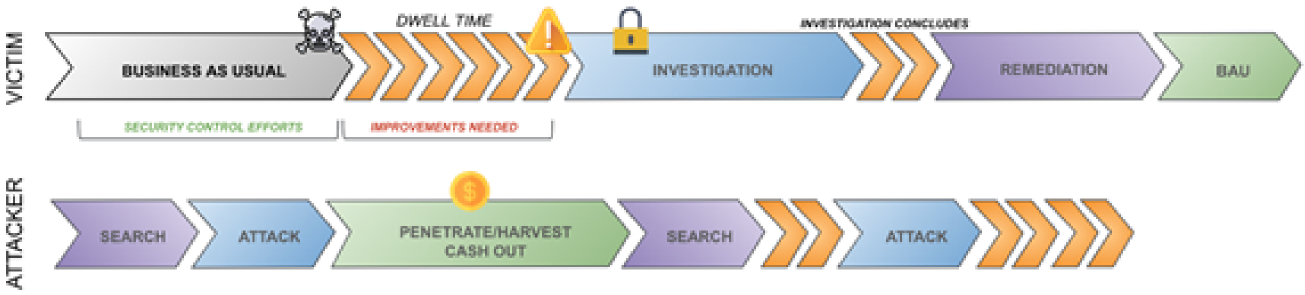
What to do in the case of an incident, how do you even define an “incident”? A typical approach today is to sit and do tabletop exercises, “What if…” scenarios are played through, exception management, and simple questions with surprisingly difficult answers are discussed.

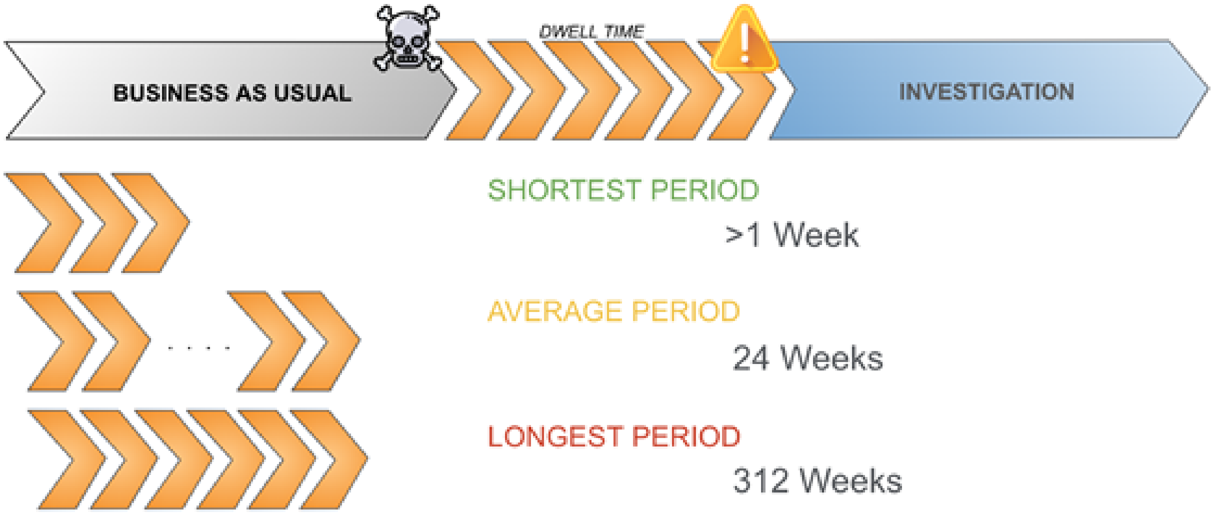
In order to protect brand and reputation during a data breach providing the right messages to customers, business partners and regulators is paramount. Incident testing should include review and sign off for communication strategies and options.


EFFICIENCY, IMPROVEMENT, OPPORTUNITY, STRATEGY, SOLUTION, IDEA, TACTICS, PROGRESS, MANAGEMENT, GOAL, DEVELOPMENT, SUCCESS, INNOVATION, PLAN,

ATTACKS AGAINST LOYALTY PROGRAMS & PLATFORMS

Within the industry it is important to start dialogue about attacks suffered by all participants, an attack against one loyalty platform could leave all the other (similar) platforms used by the loyalty customers exposed. In a 2019 article InfoSecurity Magazine claimed that two in every three users reuse passwords between websites; this must be of specific concern to the loyalty industry because this changes the attack vector used if valid credentials are used to access customer accounts.





SUMMARY

Loyalty programs and platforms are an interesting target for criminals as the pay-out of a successful attack is immense. Unfortunately, criminals know this, and organizations are having their loyalty efforts being constantly attacked.

As mentioned above, your organization needs to understand the anatomy of a data breach and the types of attack to defend from, and have an incident response plan in place.

We recommend scanning your transactional and loyalty program websites for any external vulnerability. And to have an extra layer of security, and keep on track with your compliance efforts, take a look at the Proactive Incident Response solution.

Foregenix Proactive Incident Response (Proactive IR), combines the threat hunting technology, Serengeti, and the team of Threat Intelligence Analysts, to monitor customers 24/7, actively scanning networks to hunt for threats in real-time, carry out investigations, take mitigating actions and reverse engineer new attacks to protect the clients’ systems. All of this is done in a ‘single pane of glass’ for maximum visibility and analysis.

This volume was written by

FOREGENIX

Foregenix, a member of the Loyalty Security Association, is a leading independent cyber security company with a focus on keeping the world's payment systems secure. With a decade of experience in the Payment Card Industry (PCI), it helps merchants, payment processors, banks and other operators to ensure they are securing their environments effectively while complying with industry security standards.

Foregenix works with clients in the Fintech, retail, e-commerce, hospitality, travel and insurance sectors, as well as banks and governments globally. Its specialists are drawn from backgrounds including law enforcement, counterterrorism, and digital security.

Foregenix is headquartered in the UK and has offices in Brazil, Uruguay, Germany, Singapore, South Africa Australia, and the USA.

www.foregenix.com