End to End Response:

Protecting Your Organization and Customers in the Aftermath of a Data Breach
2016 recorded an all-time high by racking up a total of 1,093 data breaches¹ in a single year. Analysis of recent breaches discovered that 80 percent of these crimes were perpetrated with financial motives² – concerted plots to defraud a business as well as its customers. Often, the information stolen during these cyberattacks belongs to a customer. Attackers leverage a customers’ credit card data, social security numbers and other personally identifiable information to make fraudulent purchases, open lines of credit, or sell to others on the Dark Web to be used for nefarious purposes.

With annual data breach incident numbers on the rise, ambiguity around legally-mandated best practices and cautionary tales of mishandled high-profile breach communications, what should businesses do? How can they ensure compliance with and respect for customer distress, considering the increasingly likelihood of a privacy incident? What steps can be taken to reduce exposure to these attacks?

Failure to consider customer assistance and recovery can prove devastating to a brand in the aftermath of a security incident. Therefore, CrowdStrike and TransUnion® have partnered to provide companies with the information they need to effectively respond to an incident. CrowdStrike offers expertise in incident response services and proactive assessments that address business cybersecurity challenges. Data Breach Services from TransUnion offer customer credit and identity protection solutions. When combined, these solutions create a robust defense against the threats posed by cyberattacks.

The statements, representations, opinions and/or content in this white paper are general and for educational purposes only and should not be viewed as advice, a replacement for contacting your professional legal and security incident advisors for required advice, and consulting all applicable laws and legal obligations implicated by a data breach. Additionally, please note that the descriptions of products and services do not in all cases represent the products and services offered by CrowdStrike or TransUnion.
Your Customer’s Personal Information Has Been Breached. How Do You Address It?

First and foremost, begin to prepare your customer communications plan. Resources and information should be clearly communicated to potentially impacted customers in a timely manner. In order to protect and restore customer confidence in the wake of a cyberattack, the following questions should be answered in the affirmative, prior to delivery:

1. Does the notification generate from a subdomain and email address that will forestall customer cynicism about the source of the communication?

2. Is the contained information clear and truthful with simple directions to products and resources that could mitigate customer impact?

3. Is the data breach notification constructed thoughtfully, with a mind toward prompt information dissemination?

Customer confidence and brand loyalty often suffer if the first point of contact is not well planned. Javelin’s 2016 Data Breach Fraud Impact Report describes the disappointing state of these communications from the customer’s perspective. Their research found that “dissatisfaction with the detail and security instructions in data breach notifications is a key factor in breach victims’ willingness to continue patronizing the breached entity.”
In addition to timely communications with your customers, ensure they have the resources they need to address any concerns or questions they may have about the breach incident. Many companies offer their customers access to a breach hotline available any time to help address their questions. Additionally, many products are now available that can help your customers prevent, detect and respond to possible risks of identity theft if their information has been compromised.

**Prevent**

Prevention solutions allow your customers to maintain control over their information and react quickly if it is compromised. For example, offering credit lock provides customers with the ability to easily lock and unlock their credit report instantly. This helps stop identity thieves from obtaining credit in their name.

Another preventative method against fraud is to encourage your customers to create strong, unique passwords. 63% of confirmed data breaches involved leveraging weak/default/stolen passwords. Tools like password managers provide the convenient service of generating strong passwords and storing them. Certain applications provide an additional layer of protection by including a 24/7 breach monitoring service, which will notify customers if an account is compromised and can update the at-risk accounts with one click.

**Detect**

Every second matters when personal information has been compromised. Detection solutions can help customers react quickly thanks to instant notification of potential fraudulent activity. For example, credit monitoring can alert your customer of changes to their credit report, allowing quick action if anything looks questionable. More detection solutions are offering a range of non-credit monitoring services, supplementing credit, multi-bureau and instant alert options. Services like Dark Web monitoring are constantly monitoring the Dark Web for compromised PII being shared or sold. Other monitoring options include non-credit loan monitoring, bank takeover and address change alerts to provide customers with more ways to detect possible identity theft in an evolving fraud landscape.

**Restore**

If your customers feel that they may be the victim of identity theft, restoration services like identity restoration and identity theft insurance equip victims with tools to confront fraud and restore their good names. Discovering fraud is stressful and restoring their identity can be taxing. Fraud resolution specialists can help guide customers through the resolution process and help mitigate potential effects of fraud.
During the busy 2013 holiday shopping season, retail giant Target experienced a massive data breach. Criminal hackers compromised the data of up to 100 million people, including some 40 million Target card holders. This was certainly bad luck and bad timing, and although the retailer took public flak for ignoring alleged warning signs, a breach is a real risk for almost any business in the 21st Century.

However, public relations surrounding the company’s recovery strategy turned out to be another nightmare. The trouble started with Target’s breach notification process. As CMO contributor Tony Bradley argued in January 2014, “if you ever find your company in the unfortunate position of needing to notify customers of a data breach and possible compromise of personal information, this is not how you do it.”

Essentially, the initial notifications were rife with what industry experts deem anti-best-practices. Among the transgressions singled out were:

1. The use of a subdomain that appeared fake to many customers - target.bfi0.com rather than target.com
2. The direction to customers to click on a nonsensical link
3. The distributed email notification that seemed to come from a suspicious email address

Bradley concludes, “in a nutshell, there is nothing about the legitimate breach notification email from Target that differentiates it in any way from a reasonably well-crafted phishing attack.”

However imperfect, the timeliness of the notifications was also widely called into question. After the holiday breach incident, Target issued a press release on January 10, 2014 announcing a second batch of pilfered data. But many customers and other impacted individuals did not receive notification that their personal information may have been compromised until January 17. The delay in timing did not go unnoticed.

Writer Jason Del Rey of Recode wondered in a January 18 post:
“Why such a delay between the initial press release and the email from the company? Was Target following the letter of the law with the timing of this disclosure? How about the initial breach notification? Was that made in the appropriate timeframe?”
In addition to developing a customer response plan, you must take both short-term actions and long-term steps to recover and secure the organization. In the short term, steps must be taken immediately to stop the bleeding of valuable data assets and preserve forensic evidence that will be useful during the investigation and remediation process. After you make it through a breach, you will need to take long-term actions that often include improving security controls, performing technical assessments and evaluating current processes to mitigate the risk of another breach.

The short-term and long-term recommendations in this document are derived from decades of collective experience by cybersecurity consultants on the front lines fighting threats daily. These recommendations can help your organization both prepare for and respond to the next targeted attack.

**SHORT-TERM ACTIONS: WHAT TO DO IMMEDIATELY AFTER AN ATTACK**

**Preserve – Coordinate – Respond**

Cyberattacks are inevitable in organizations with sensitive data. When responding to these attacks, every detail is critical in protecting the business’s reputation and preserving the customer’s trust. The limited time to react during a breach requires that organizations have a well-thought-out and strategic approach, allowing them to perform coordinated internal response efforts and swift decision making. To effectively react when notified of a breach, we believe your organization should preserve, coordinate and respond.

**Preserve**

Do not disconnect!

Many targeted data breaches go on for months before detection. When a compromised system is hastily disconnected, it is highly probable that the attacker will compromise additional systems to establish new forms of persistence that may go undetected, or he may have already prepared backdoors for these situations. Attacker behavior is likely to change and a game of “whack-a-mole” may ensue once he knows he has been detected. If a computer must be disconnected, ensure that a forensic image (including a memory image) of the system is preserved prior to disconnecting power.

**Collect log data**

Log data is often crucial in determining how the incident occurred, when the incident began, the range of systems affected and the data that was accessed or targeted. You must validate that all centralized host-based and network-based logs are being preserved, and that backups of critical servers are available. The incident may have started over a year ago, making all rolling logs valuable, regardless of age. The attacker may also be quick to clear any unprotected logging if he feels he has been discovered.
Coordinate

Establish internal communications

Formulating a response to a data breach requires internal communication and coordination within your organization. At a minimum, key players from IT, security, legal and public relations must be kept informed of the status of the data breach. Each player fulfills key functions which enable the investigation, the formulation a response and the communication with regulatory agencies as well as customers. In some cases, if there is reason to believe internal network communications may be compromised, out-of-band communication and collaboration channels should be established and utilized by the response team.

Engage an incident response services company

Even large security teams often need surge assistance early in the incident response cycle and during remediation efforts. Establishing a retainer and getting initial paperwork in place can minimize delays to your investigative efforts when help is required. Companies that do not have a contractual relationship in place with an IR firm in advance of a breach, typically take two to three times longer to get the support they need after discovery. Consider proactively partnering with a company that can provide all the different services needed in the short and long-term. This will help ensure cohesive communication and planning throughout the entire process.

Understand legal requirements

To this point, the creation and enforcement of minimum notification standards has been a state’s rights issue. Forty-seven states, Washington D.C., Puerto Rico, Guam and the U.S. Virgin Islands, have some form of data breach notice requirement. It is important to ensure your organization understands these requirements.
Respond

Monitor workstations, servers and internet egress points

Legacy signature-based antivirus endpoint offerings do not provide the real-time visibility into activity on your endpoints, which is necessary to detect and stop attacks. An endpoint detection and response (EDR) solution can provide the visibility that is crucial in stopping an attack before it starts. Deploying a cloud-based EDR solution also accelerates recovery time after a cyberattack. Ensure that damage is limited, data exfiltration has stopped and remediation can begin by leveraging an endpoint technology that enables security staff to detect, prevent, record and search in real-time to stop targeted attacks before they can cause damage. Monitoring internet egress network traffic provides enhanced coverage for unmanaged endpoints and provides additional context to an attack.

Scope and investigate the incident

Proper scoping of an incident during an investigation is critical to concentrating resources on containment and eradication efforts. Without an accurate scope, attackers may be able to maintain their presence within an environment. Responders will need to conduct endpoint and network forensics to identify active malware in your environment, the source of attack and attacker attribution. Endpoint forensics will help determine how many systems have been accessed or compromised, which data may have been accessed, how long the incident has been occurring, the initial attack vector, persistence mechanisms in your environment and exfiltrated data. If a cardholder data environment has been affected, you may need to bring in a PFI-certified forensic firm approved by the PCI Security Standards Council to investigate.

Remediate the attack

Remediation efforts should be coordinated in a way that completely removes the attacker from the environment and limits his ability to return in another way. Isolate critical systems (i.e., point of sale, CRM, inventory management) from the broader network and block access to the adversary’s command and control infrastructure. Remove and completely refresh infected hosts. Perform credential resets where needed. Then, assess additional measures to harden the environment based on the findings of the incident response investigation and security review.
Govern – Secure – Operate

Today’s sophisticated attackers will not limit their tactics and techniques to known malware and exploits. Therefore, conventional malware-based protection is insufficient to stop targeted, persistent attacks. Careful consideration and long-term strategic planning should be devoted to preparing for these attacks. Address threats proactively under the pillars of govern, secure and operate.

Govern

Be proactive: have a data breach response plan in place

A data breach plan should establish best practices, define key roles and responsibilities, and identify process for the organization’s response efforts. Plans should focus on both internal efforts to restore data and systems’ confidentiality, integrity and availability, as well as external requirements like contacting insurance carriers, law enforcement, regulators, customers, vendors and public relations teams in response to the loss of potentially sensitive data. This is not just a paper exercise, an effective response plan requires that all parties involved understand their roles within the process and should include regular vetting and updating as people, process and technology changes occur.

Empower a cybersecurity risk management program

The identification, evaluation and prioritization of cybersecurity risks enables you to foresee issues and proactively determine appropriate responses. Decisions around planning and prioritizing security controls should be informed and supported by a mature cybersecurity risk management program.

Develop a cyber strategy and roadmap

Once you understand the risks to your organization and the gaps within your cybersecurity defenses, set targets for maturity and goals to mitigate risk. These efforts should be prioritized along with your existing plans as part of a strategic roadmap for improving overall cybersecurity maturity.
Identify and classify assets

Organizations that try to protect all of their cyber assets equally often fail to protect what is most important to them. First understanding and then focusing security controls on where the most critical and sensitive data and assets reside within the environment is essential to proper cyber risk mitigation strategy. This inventory should inform efforts to concentrate security resources and restrict access to your organization’s most critical data.

Conduct regular education and awareness training

Educating your employees and increasing employee awareness should be part of your ongoing proactive security efforts. Your employees can be human sensors that identify and report potential incidents, such as a targeted spear-phishing or social engineering campaigns. Employees throughout the organization should be aware of the importance of good security and know what to do if they suspect a breach.

Establish a metrics and reporting function

An organization cannot protect what it cannot measure. Therefore, cybersecurity controls and objectives should be continuously monitored and reported to key stakeholders. These metrics should be organized in a meaningful way to quantify risk and inform decision making. Regular metrics will give decision-makers the ability to measure progress and set goals for improvement, as well as prioritize security initiatives to maximize return on investment.

Augment your IT/security team with security experts

We live in an age where cyber talent is hard to find and expensive to retain. Professional security consultants utilize the latest cyber threat intelligence either via feeds or other reporting sources. This enables them to access the latest threat actor tactics, tools and procedures (TTPs) which can inform their investigation of an incident. It also means they will have a greater ability to attribute a cyberattack to specific threat actors.
**Secure**

- **Identify, isolate, and log access to critical data**
  Focus your limited resources on those areas of the network that are most critical to your business. Determine where your most sensitive data or networks are located and implement increased logging and network monitoring. Actively monitor network access and conduct frequent log reviews.

- **Implement centralized logging**
  Having robust log aggregation and retention can support a data breach investigation by assisting responders in correlating certain events and developing an incident timeline. DHCP, DNS, Active Directory, server event logs, firewall logs, IDs and Proxy Logs should all be stored in a protected, centralized system that is time-synchronized and easily searchable. Allocate resources to perform regular log analysis and stress test your logging process via tabletop intrusion exercises.

- **Consolidate internet egress points**
  In the event of an intrusion, monitoring egress points is also a critical part of identifying attacker activity. All connections to the internet from your corporate environment should be monitored to identify data leaving the network. The fewer egress points there are to monitor, the easier it is to detect malicious activity and the more cost-effective they are to monitor.

- **Apply operating system and third-party application updates**
  Patching operating systems and third-party applications is one of the most inexpensive, yet effective, ways to harden a network. It allows your employees to focus on detecting advanced adversaries. Build a strong patch management process and ensure critical security patches are installed as soon as possible. If you have legacy operating systems or software packages in your enterprise, develop and implement an upgrade plan.
Manage user credentials rigorously

Media coverage is littered with companies that did not adequately protect their user accounts. Passwords are consistently reported as being for sale on the Dark Web. If your organization maintains user accounts, audit your password storage functions. Solutions exist to make password management straightforward and secure by providing strong encryption and salted hashing, but they require proper implementation.

Protect critical systems, including those outside your network perimeter

As the workforce becomes more mobile, centralized intrusion detection, file sandboxing and other security safeguards are not always capable of protecting all endpoint devices at all times. Advanced adversaries often compromise devices outside of your perimeter, taking advantage of the endemic poor security of other networks. Ensure that your endpoint solutions provide the same protection regardless of the location of the device.

Require two-factor authentication (2FA) at login

Remote access into your network should always require two-factor authentication. Consider also requiring two-factor authentication for sensitive administrative accounts. Out-of-band authentication methods like SMS and soft tokens are commonplace, widely accepted by users and relatively easy to implement with the prevalence of smartphones.

Change default passwords

One of the simplest attacks is to use a default password that is shipped out-of-the-box by a vendor. Internet of Things (IoT) devices are commonly highlighted for this vulnerability, but the attack scope is much broader. Default passwords, especially for hardware devices (e.g. Wi-Fi routers), can allow direct access to critical data. Extra care should be taken to require strong passwords for all users, including default or built-in accounts.
Operate

Train like you fight

Testing incident response (IR) readiness with tabletop exercises offers immense benefits when it comes to being operationally ready for a data breach. Working through roles, responsibilities and the steps of a complete IR plan prepares a team for action and quickly identifies any weaknesses in your plan, including processes, data collection efforts and team capabilities. This exercise may be helped by working with an IR services team with real-world expertise and up-to-date scenarios.

Conduct regular red teaming exercises

While still an integral part of an overall security program, simple vulnerability scans are not enough to evaluate your technology security position. Test your organization’s ability to stand up to the actual tools, techniques and procedures used by the adversaries who actively target your industry. These exercises will give you a better understanding of your ability to prevent, detect and respond to targeted attacks.

Leverage cyber threat intelligence

You cannot focus on all threats at once. Train responders to identify the most relevant threats by leveraging cyber threat intelligence, which should be considered as important as other forms of business intelligence. Subscribe to vulnerability intelligence feeds and reporting, such as Falcon Intelligence™, and ensure continuous monitoring via security platforms with the ability to automatically ingest intelligence data.

Encourage information sharing

Organizations that are better able to detect and respond to breaches generally have integrated fraud and IT security departments. Encourage regular information sharing in your organization. IP addresses and system names associated with fraudulent transactions can be the indicators needed to identify other suspicious network activity or, ultimately, a data breach.
CONCLUSIONS

Some industry experts explain a business’s necessary cultural changes in the aftermath of a data breach incident with a simple rhyme: sophistication follows humiliation. CrowdStrike and TransUnion offers your organization a real opportunity to get in front of the infrastructure, brand and customer damages associated with a cyber-attack.

CrowdStrike Services stops breaches by providing pre- and post-incident response services to proactively defend against and respond to cyber incidents. A team of cyber intelligence professionals, incident responders and malware researchers form a group of internationally recognized authors, speakers and experts who have worked on some of the largest, most publicized and challenging intrusions and malware attacks in recent years. CrowdStrike stops breaches. Call (888) 512-8906 to learn more.

Your organization must also be ready to respond to customer concerns when every second counts. Security threats do not need to bring business to a halt. Should the unthinkable happen, be ready to help victims confront fraud and restore their good names. Your organization deserves a specific, customer-focused strategy that helps protect and restore brand confidence. Start the conversation by emailing TransUnion at databreach@transunion.com, or call 800-719-1636.

¹ ITRC website 1/19/2017
² Verizon, 2016 Data Breach Investigations Report
³ https://blog.pcisecuritystandards.org/closer-look-the-pfi-programme
⁴ Gemalto, 2016 Data Breaches and Customer Loyalty report
⁵ http://www.iii.org/fact-statistic/identity-theft-and-cybercrime
⁶ 2016 Data Breach Fraud Impact Report, Javelin Strategy & Research
⁸ The Huffington Post, “A Look Back at the Target Breach,” June 6, 2015