Research Report

A Trip to the Cyber Range: An Immersive Response and Strategic Planning Exercise

Introduction

Does your organization have a comprehensive plan in place to deal with major data breaches? Does your organization have the right tools and the right policies and procedures in place to isolate the cause of a breach and shut it down? Does that plan include ways to analyze breaches; ways to assess the damage; and ways to interact with the onslaught of press, customers and regulators who will demand answers and assurances afterward? Do your employees know their exact responsibilities should a breach occur? These are the types of questions that business and information technology (IT) executives will find themselves asking should they visit IBM's new X-Force Command Center Cyber Range.

I recently had the opportunity to visit IBM's Cyber Range in Cambridge, Massachusetts. I After sign in, I was escorted to a large conference room that featured over 30 displays– in an imaginary immersive security operations center. Two IBM security faculty immediately started my lesson in *cybersecurity breach response* with an overview of the Cyber Range, followed by a discussion of goals and objectives. The individual who guided me through the exercise explained a bit about typical security challenges, and then detailed how the security drill would work. Essentially, I would be put in charge of a fictitious company and I would be expected guide the company's response to a security breach in which customer data was published on the web for all to see.

And then, all heck broke loose. The exercise started with a blindside – a crisis situation I was not prepared to handle. (I'll not describe the blindside – it would ruin the fun for future attendees – but trust me, it catches you off-guard).

As I attempted to deal with the crisis, a litany of questions jumped into my mind:

- What data has been breached and published?
- Was the leak plugged?
- Was it internal or external?
- At what point do I address the media, and what do I tell them?

As the crisis unfolded, I was asked in rapid fashion to handle the customer outcry, the press inquiries, and to deal with regulators. Again, this is another activity that I'll be scarce on details with in order to maintain the element of surprise – but let's just say this: as you go through this exercise you realize that a plan should have been put in place to handle a crisis like the one I was facing ***BEFORE*** the situation occurred. After around forty-five stressful

minutes, the exercise drew to a close with a final press interview, which IBM confirmed that I handled well.

> ***Looking back at the experience I realized that there has got to be a process in place, supported by the right security tools, the right project management/process flow tools -- and supported by specific individuals assigned to handle a wide variety of tasks that must be addressed should a breach occur.***

The Tools

As I watched the exercise unfold, I was shown a lot of tools that were used to identify the source of the breach; to analyze internal behaviors; to manage the process flow; to assess the potential damage in terms of regulatory fines; and more. I have seen most of IBM's security product offerings in demonstrations at various conferences – but I had never seen them all in action, working together in a seamless, integrated fashion. Impressive.

I have written about several of IBM's security tools over the past few years (see this report, this report and this report) – so I had a working knowledge of the features and functions of the respective products. I was most impressed by IBM's Resilient environment, an incident response platform that provides a means to work collaboratively through the breach process in an organized, project management-like fashion.

> ***IBM Resilient offers a series of working "playbooks" that help guide executives through all of the steps of the breach process. Activities can be set up in advance, with contact names, a description of the task that must be performed, and the name and contact information for individuals assigned to execute tasks. This software can even extrapolate a company's financial exposure in terms of regulatory fines (and remember that if certain tasks aren't executed in certain time frames, fines go up exponentially).***

IBM's i2 visual investigation and analysis tools also played a major role in the breach analysis process.

As I claim in one of the above-mentioned reports, I contend that cognitive computing is on a path to become pervasive in the security community. During the course of the breach exercise, IBM's cognitively-enabled QRadar was used to formulate a "threat query" which it forwarded to IBM Watson for Cyber Security for additional analysis.

Watson searched its corpus of structured and unstructured data – and it searches for other threat entities – and let me know about threats that may have been related to the breach that I was attempting to manage. The information gleaned by Watson for Cyber Security was refined by QRadar – using insights identified by QRadar, by Watson for Cyber Security and by the security administrator. In a relatively short amount of time these tools enabled me to identify the source of the breach.

IBM's BigFix Detect was also used in the analysis process. This program is an endpoint detection and response (EDR) environment designed to identify malicious behavior at the point where external threats begin. When used with Watson for Cyber Security, the combo

can deliver targeted remediation to endpoints that have been compromised quickly – within minutes – helping cut off cyber attacks.

> ***Not that IBM did not overtly try and sell me on any of these products – the company merely showed what needed to be done during a cyber attack, then used the tools at its disposal to manage the situation. Interestingly, IBM did not mention any of the services that it could use to help me implement a breach response plan or formulate a comprehensive security plan. This was likely due to the abbreviated nature of my visit – the exercise can run anywhere from 4-8 hours, whereas I could only devote 60 minutes to the exercise.***

Service Offerings

Though IBM did not describe its services, I think those offerings are worth mentioning here. I know from previous research that IBM's security services fall into 7 categories:

1. Data and application security services;
2. Offensive security testing;
3. Incident response and intelligence services;
4. Identity and access management;
5. Infrastructure and endpoint security;
6. Security strategy, risk and compliance; and,
7. Security intelligence and optimization).

As background, IBM's data and application security services help secure data and applications. The company's data security capabilities are based on its Guardium offering, which provides data and file activity monitoring, threat detection analytics, vulnerability and more. The company also offers application security on cloud consulting services. IBM's offensive security testing services include a programmatic approach to security testing of all types, including human, process, hardware, IoT, application and infrastructure.

The IBM X-Force Red portal helps provide visibility into asset vulnerabilities and offensive security reporting facilities. IBM X-Force Incident Response and Intelligence Services are backed by an organization that helps prepare clients to instantly respond to security incidents. The services offered include a proactive retainer program known as IBM X-Force IRIS Vision Retainer and cybersecurity consulting services to deal with active threats.

IBM's identity and access management services protect against breaches, and include identity and access strategy and assessment, cloud identity and insider threat protection services. IBM's infrastructure and endpoint security aim at transforming existing email, Web, network, server and endpoint environments into modern, well secured environments through managed security services, cloud security services, network protection services (such as a managed firewall service), and through managed detection and response services.

The company's security strategy, risk and compliance service aims at meeting regulatory requirements. This service makes recommendations for the better management of risks, compliance and governance – and includes IBM's GDPR privacy service.

IBM's security intelligence and optimization service aims at proactively detecting and prioritizing threats. This service is designed to assist clients throughout the Threat Management lifecycle, including strategic security operations center planning and deployment, 24x7 threat monitoring and analysis, rules and use case management, and closed-loop intelligence processing. This offering also includes services from the IBM X-Force Command Centers such as the IBM X-Force Hosted Threat Analysis Service. Managed SIEM and strategic SOC consulting are two important services in this area.

Summary Observations

I thoroughly enjoyed my visit to IBM's Cyber Range. It was a fun, immersive and extremely informative exercise—a great way to spend an afternoon in Cambridge other than strolling Havad Yahd.

When I started the exercise, I had no idea what to expect. It could've been like other briefings – typically discussions of a vendor's strategies, products and services. But IBM has taken this process to the next level, making it an immersive learning and teaching experience. I "got into" the exercise big time, marveling at the technologies I had at my disposal. IBM's suite of integrated tools made it easy for me to ascertain the source of the problem and respond rapidly, in an organized fashion, to a data breach.

Due to time constraints, I could not finish the full experience. I was told that it can last four hours, and that teams of security personnel are provided learning materials and planning materials that they fill out in real time to help them figure out how to build their own security strategies. The Cyber Range is really an educational opportunity made fun through the use of immersion technologies.

I loved the parting words of the lead faculty member as he concluded our time together. "The Cyber Range is where security best practices meet. It's where the game of CLUE converges with security process flow on a Disney roller coaster ride." From my perspective, he's 100% right – it's fun, it's exciting and it is a fantastic learning experience for those looking to IBM to help them build a comprehensive, fast-response security breach plan.

Clabby Analytics
http://www.clabbyanalytics.com
Telephone: 001 (207) 239-1211