Global Information Assurance Certification Paper

Lessons Learned from Treatment of Trauma in Individuals and Organizations Under Repeated Cyber Attacks

GIAC (GSEC) Gold Certification

Author: Vanessa Pegueros, vpegueros@gmail.com
Advisor: Rob Vandenbrink
Accepted: June 6, 2016

Abstract

There has been significant research relative to the impacts of trauma on human beings and the associated treatment of that trauma. With the increasing frequency of cyber-attacks and associated breaches, people within organizations are experiencing similar traumatic effects felt by victims of a more physical attack or incident. There are significant parallels between the impacts of cyber-attacks on organizations and the impacts on individuals experiencing some form of trauma. There are key lessons to be learned from the treatment of trauma victims and the techniques to help organizations become more prepared and resilient relative to cyber-attacks. With the continued escalation of cyber-attacks, organizations should be working to implement solutions beyond just security technology and look to the process and people elements of the solution.

1. Introduction

People in security are often asked, "how do you sleep at night?" By the very nature of the question, it is assumed that being an information security professional is stressful. Most security professionals, especially those involved with security operations and incident response would agree that their job is dynamic and unpredictable. While this has impacts on the individuals themselves, there are also larger impacts to the organization that comes under attack. Managing and avoiding the long-term impacts of trauma to the organization is key to survival in the current threat environment. There has been significant research conducted on the treatment of individuals who have experienced trauma and valuable lessons can be learned from the research relative to "treating" the individuals in the organization who experience cyber-attacks.

2. History of Cyber Attacks and Trends

Information warfare, asymmetric warfare, the threat of being overwhelmed is commonplace within the field of information security. Based on Figure 1, over the past 9 years, cyber security breaches have increased 498% and by all forecasts will continue to grow both in volume and sophistication.

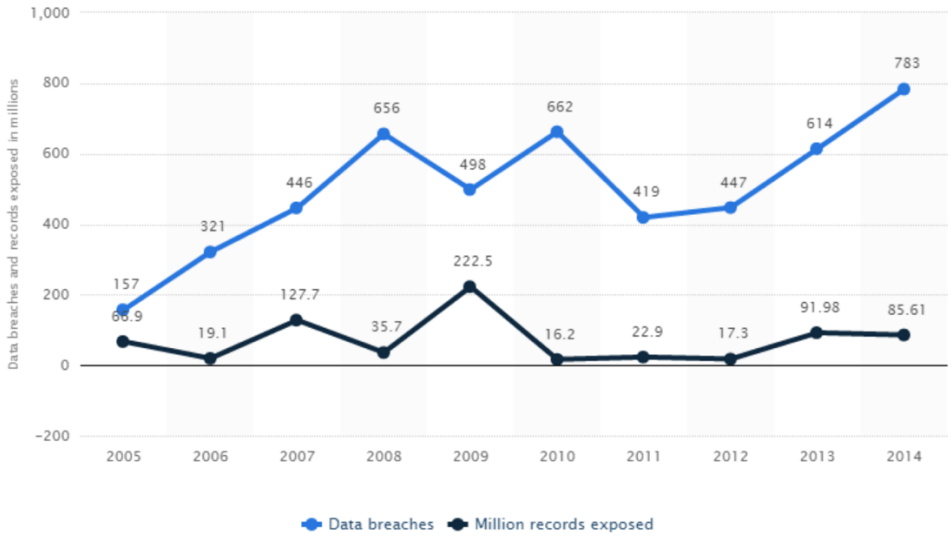

Figure 1. Growth of Data Breaches. Reprinted from Digital Guardian, by D. Lord, 2015, Retrieved from https://digitalguardian.com/blog/history-data-breaches.

The costs to the company of a breach are numerous; based on the author's experience these include both direct (regulatory fines, lawsuits, customer notification, remediation, additional audit and security costs) and indirect (brand impact, staff departure, lost employee productivity). "Home Depot spent approximately $43 million per quarter on remediating the payment data breach. Target spent a whopping $148 million on remediating the impacts of its credit card breach" (Cser, Andras, Ferrara, Ed, & Kindervag, John, 2015). It is important to understand the trends relative to these costs, as an example, costs related to fines from consumer privacy organizations including the FTC, FCC, and EU Data Protection agencies are increasing. The EU General Data Protection Regulation (GDPR) allows fines of 4% of global revenue or 20M euro, whichever is greater (SC Magazine, 2015). Additionally, companies have begun to experience both significant brand impact as well as organization structure impact as in the case of Target losing both its CEO and CIO. Company Boards are coming under close scrutiny and consumers/employees are organizing class action lawsuits.

A cost to companies that has not been explored sufficiently is the psychological impact including the impact to the employees of the company that has been breached or coming under consistent cyber-attack. As organizations increasingly come under cyber-attack and experience painful breaches, there are manifestations of significant trauma, not dissimilar to a human who comes under attack and experiences the effects of trauma.

Some of those impacts are manifested in the firing of top-level executives, reorganizations, clumsy corporate communications, reacting and spending too much to fix the problem and of course the anxiety felt by the organization at all levels that it "could happen again." The author is of the opinion that in an effort to control the impact of the attack or breach and thus prevent further trauma, there will be a tendency to suppress further "bad news".

In all our effort to define the process, tools, and technology relative to incident response, we seem to have ignored the very key impact the current breach environment has had on organizations and their "mental health" relative to incident response. Understanding the human response to danger and the treatment of individuals with trauma, provides insight into how we can improve how our organizations can stay healthy and improve their capabilities around incident response.

3. Human Response to Trauma

The human body is an incredible incident response system organized to survive, a model information security teams should spend more time understanding. It is important to understand how the human individual brain operates during time of danger. In order to ensure survival, the brain has five main functions (Van Der Kolk, 2014):

1. Generate internal signals that register what our bodies need such as food, rest, protection, sex, and shelter
2. Create a personal map of the world to point us where to go to satisfy those needs
3. Generate the necessary energy and actions to get us there
4. Warn us of dangers and opportunities along the way
5. Adjust our actions based on the requirements of movement

According to the Paul MacLean Triune Brain Model, there are 3 key parts of the human brain (Levine, 2010):

Level 3: Neocortex level: Thinking, conscious memory, symbols, planning and inhibition of impulses
Level 2: Limbic, mammalian level: Feelings, motivation, interaction, and relationship
Level 1: Reptilian (brain stem) level: Sensation, arousal-regulation and initiation of movement impulses

In a level 1 response, the sensory input from our ears, eyes, nose, touch acts to provide information to the thalamus. The thalamus passes the information on to the amygdala to interpret the criticality of the input. If it is determined that there is a threat to the body, the amygdala sends information to the hypothalamus to secrete stress hormones and begin physical response to the threat. This level of response happens in the fastest amount of time and involves very little processing.

In a level 2/3 response, there is a much more conscious and refined response by the brain, however, the response time is slower. "At this response level the thalamus communicates through the hippocampus and anterior cingulate to the neocortex (the rational brain)." (Van Der Kolk, 2014). When a higher-level response is enabled, the individual has the ability to make better thought out decisions. "Executive capacities of the prefrontal cortex enable people to observe what is going on, predict what will happen if they take a certain action, and make a conscious choice" (Van Der Kolk, 2014). "Being able to hover calmly and objectively over our thoughts, feelings, and emotions and then take the time to respond allows the executive brain to inhibit, organize, and modulate the hardwired automatic reaction preprogrammed into the emotional brain" (Van Der Kolk, 2014).

In the event of a traumatic event there are common symptoms that the individual exhibits including (National Center for PTSD, 2015):

1. **Reliving the event (also called re-experiencing symptoms)**
   Memories of the traumatic event can come back at any time. You may feel the same fear and horror you did when the event took place.
2. **Avoiding situations that remind you of the event**
   You may try to avoid situations or people that trigger memories of the traumatic event. You may even avoid talking or thinking about the event.
3. **Negative changes in beliefs and feelings**
   The way you think about yourself and others changes because of the trauma.
4. **Feeling keyed up (also called hyper arousal)**
   You may be jittery, or always alert and on the lookout for danger. You might suddenly become angry or irritable.

When considering that humans will tend to avoid situations that remind them of the traumatic event, this partially explains an organization's response to not talk about the attack or breach. In some cases, information will be purposely concealed relative to the breach in an effort to do "damage control". Humans have a very natural response to unpleasant feelings or experiences, they try to avoid them. "To facilitate survival in an increasingly complex and socially mediated world, a new mammalian adaptation evolved: feeling states. Feelings are never

neutral; they exist along what is a called a "hedonic continuum" designating affective spectrum from unpleasant to pleasant." (Levine, 2010)

In the case of continued and long-term trauma, numbness will begin to be experienced by the victim. "In response to the trauma itself, and in coping with the dread that persisted long afterward, patients had learned to shut down the brain areas that transmit the visceral feelings and emotions that accompany and define terror." (Van Der Kolk, 2014) With the numerous and constant cyber incidents impacting consumers such as identity theft, ransomware as well as corporations experiencing growing threats and impacts, numbness is setting in for both the consumer and corporations.

Another potential response to a threat of trauma is denial. "Some people simply go into denial. Their bodies register the threat, but their conscious minds go on as if nothing has happened." (Van Der Kolk, 2014) This is a common behavior being demonstrated by executives today as their information security teams try to inform them of the threats but denial sets in and are met with responses such as "that won't happen to us or why would anyone want what we have". Based on interviews with former Home Depot security team members, it is clear that management did not consider the security needs a priority, "several former Home Depot employees said they were not surprised the company had been hacked. They said that over the years, when they sought new software and training, managers came back with the same response: "We sell hammers." (Creswell and Perlroth, 2014).

6. Lessons Learned from Trauma Research

In the research done by Pross and Schweitzer it is concluded that, "Lack of structure and chaotic environment foster stress in teams and disrupt the organization; this is experienced as a reenactment of trauma." (Schwietzer, Sonja & Pross, Christian, 2010). By the very nature of cyber security threats in today's environment, it is clear that security teams and incident response teams are feeling chaos, uncertainty, unpredictability, and lack of control. All these factors are symptomatic of the makings of traumatic response within an individual and symptoms of trauma include burn out, isolation (us vs. them), paranoia, a black and white approach to situations and

decision making, rehashing of the bad events (Fear Uncertainty & Doubt) and an obsession with attribution.

Pross et al. further point out that organizations with low stress and conflict levels have several key attributes including, "good leadership delegating tasks and responsibilities, clear definition of roles and competence…extensive ongoing professional training, and a common approach to the job" (Schwietzer, Sonja & Pross, Christian, 2010). Additionally, they noted, "Organizations and their leaders should place great emphasis on self-care, meaning limitation of workload, avoidance of overwork, the opportunity to rotate into non-trauma related work, time or sabbaticals, and a culture of sociability in the team that may include team parities, leisure activities, and retreats." (Schwietzer, Sonja & Pross, Christian, 2010).

According to Levine, it is important to achieve both a successful escape and achieve empowerment in order to avoid the long-term impacts of trauma. "Effective treatment is a matter of helping individuals keep the "observing" prefrontal cortex online as it simultaneously experiences the raw primitive sensations generated in the archaic portions of the brain" (Levine, 2010).

In a situation where successful escape and empowerment are replaced by unsuccessful escape and an experience of fear and helplessness, there will be long term traumatic impacts that will take root in both the individual and the organization.

- Immobility
- Arousal
- Running
- **Successful Escape-→ Unsuccessful Escape**
- **Empowerment→Experience Fear and Helplessness**

A fairly recent example of how this execution of trauma if occurring in the cyber world is quickly evolving problem of malware called crypto ransomware. From the author's experience with ransomware, it infects a user's computer and promotes **unsuccessful escape** by encrypting the data of the user and preventing the user from accessing that data unless they meet the demands of the attacker. The victim is held hostage until the demands of the perpetrator are met, essentially preventing successful escape and promoting a sense of helplessness. "Every business

and consumer using the Internet is a potential target for ransomware perpetrators, although small and medium-size businesses (SMBs) have become particularly easy marks"(Woods, 2016). Additionally, the technical sophistication of crypto ransomware is evolving as criminals realize the effectiveness of this attack.

Recently, a new form of ransomware has emerged called Jigsaw crypto-ransomware. The ransomware is engineered to prevent escape and penalizes the victim for not reacting faster in the manner desired by the criminal. "The ransomware deletes one file after the first hour has passed and then increases the number of files it deletes in every 60-minutes cycle. If no payment has been made within 72 hours, all remaining files will be deleted." (Constantin, Lucian, 2016). This significantly increases the fear and helplessness by escalating the consequence. While there is a solution to this particular form of malware, it requires the user both have knowledge of the solution (escape route) and take the time implement it. It is somewhat ironic that the technology used to protect data, encryption, is now being used to exploit data. In order to combat this growing problem, it is important to look at the current approach to incident management and response in order to identify areas for improvement.

7. Current Incident Management Thinking

The primary goal of incident management is to maintain business continuity in the event of a cyber-attack. "Incident handling is the action or plan for dealing with intrusions, cyber-theft, denial of service attacks, malicious code and other events" (SANS Security 401, "Defense in Depth", 401.2). There are many frameworks that outline the Incident response lifecycle. The NIST Incident Handling framework (Paul Cichonski, Tom Miller, Tim Grance, and Karen Scarfone, 2012) is a useful example:

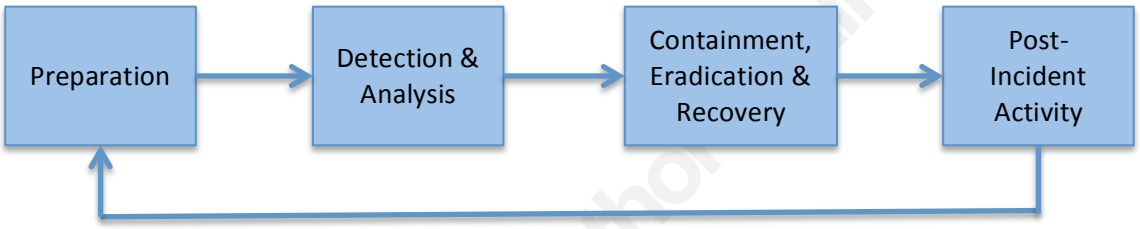

Figure 2: Incident Response Lifecycle: Computer Security Incident Handling Guide, NIST 800-61 revision 2

Preparation includes ensuring that there is a documented incident response process and all key stakeholders understand their roles and responsibilities in that process. Key stakeholders should be trained in the incident response process and participate in practice sessions such as table top exercises (Paul Cichonski, Tom Miller, Tim Grance, and Karen Scarfone, 2012) Preparation also includes understanding your current state of your environment including the vulnerabilities in your environment at both an application and infrastructure level. This is critical as a preparation step since it will allow you to quickly assess the potential weaknesses relative to specific attack. Inventory at both an asset level and ownership level is also very critical during a response activity as a system and its associated owner should be able to be quickly determined. Finally, an active intelligence program is critical to understanding the external environment and giving some predictive information relative to pending attacks.

Detection involves the implementation of technology (system/application logs, device logs, intrusion detection systems, performance dashboards, etc..) as well as processes (e.g. customer problem escalation) to identify events that are considered malicious or abnormal (Ranum, 2015). There are situations where issues are detected through non-technical means

such as customers calling into customer service. Once an event is detected the security analyst must determine whether the issue is of a severity justified to trigger the incident response process.

During containment, eradication, and recovery, the security analyst should work to isolate and eliminate the source of the incident (Paul Cichonski, Tom Miller, Tim Grance, and Karen Scarfone, 2012). This may take on many forms in terms of actions including taking the infected system offline, reimaging the computer/server, blocking outbound communication to the command and control network, determining what other systems patient zero interacted with and analyzing those systems, scanning the environment for other instances of the malware including backups, and taking a forensic image of the infected systems. Additionally, in this phase a determination will need to be made on whether to involve law enforcement. A company may also consider bringing in an outside firm to assist in the forensic work, especially if the internal resources are limited. Finally, in the recovery phase, systems would be restored from a trusted source and put back online.

From the author's experience, post incident activity includes items such as final documentation and reporting as well as holding a lessons learned session with all key stakeholders involved in the incident. During a lessons learned session, the following should be considered:

- Gaps in policies, processes and technologies
- Gaps in skills/knowledge of those involved in the incident
- Areas of miscommunication
- Identification of gaps in incident team members (were groups missing)

Based on my experience and discussions with vendors and various security teams, there is a great amount of energy that is focused on the Detection & Analysis as well as the Containment, eradication and recovery phases in today's environment. There are several reasons for this focus. One of the more powerful reasons is that technology is involved in these two phases and there is always a tendency to focus on technology as the solution to the larger problem within information security teams. Additionally, there is a lot of focus from new vendors in this space powered by a healthy influx of venture capital dollars.

More recently, there has been increased discussion around the importance of incident response exercises and the other aspects of the preparation phase; however, more needs to be done in this area. Additionally, once the incident "over', the Post Incident activity is very weak as most on the incident team are just glad to be done with the incident and move back into normal operations. This is a natural response and part of the "successful escape" which lessens the traumatic impact. The team completely misses the opportunity for organizational learning and continuous improvement.

Based on the author's experience, another important factor to note in today's world of incident response, is that Executives and Boards are creating too much distraction for the teams. Their own trauma response related to the current threat environment is compounding the stress levels of the security and incident response teams. In an attempt to quell their own anxiety relative to a situation, they ask very pointed and specific questions to the teams such as Company XYZ just got hacked as a result of vulnerability ABC, "are we vulnerable to that too?" This inevitably spins the security team into crafting a response which may require significant effort to find the answer and sidetracks the team's focus away from resolving potentially greater security risks.

8. Framework and Recommendations

As previously noted, successful escape is the key to avoiding long-term traumatic impacts. The key criteria to ensure a successful escape and thus avoid trauma include the following key elements:

- Efficient communication paths
- Providing space to have a higher level response
- Physical health
- Having an escape plan/route

It is important to consider each of these elements when developing a strategy for a more robust organization capable of preventing long-term trauma. In addition, it is useful to draw

parallels between how the brain functions during a traumatic event and how organizations should equip themselves to respond effectively during a cyber-incident.

As can be seen from Figure 3 below, the brain has various levels of response beginning with the reptilian response and moving up the stack from a reactive to thoughtful and aware mode. There are two options for regulating the brain response, control from the top down or control from the bottom up. With a human being, you may achieve more effective regulation through techniques such as meditation and yoga (Van Der Kolk, 2014). People on taught techniques around breathing (e.g. box breathing) to assist them in stressful situations with the goal to create a top down response versus a bottom up response. *Organizations too should strive to get out of the reptilian mode and move up the stack relative to response.*

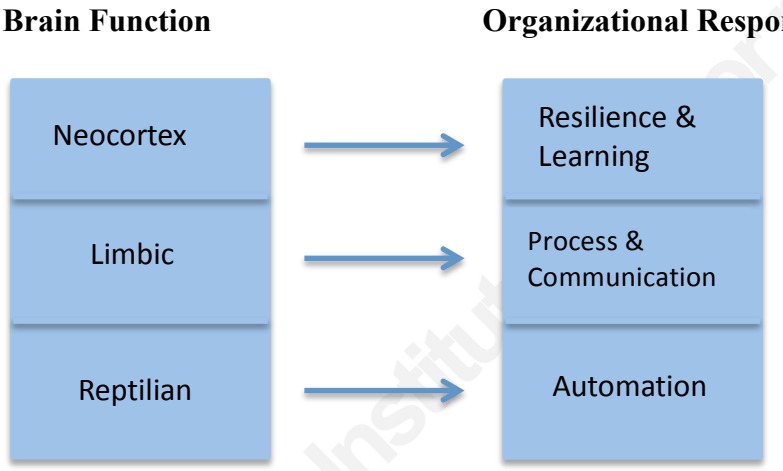

Figure 3: Mapping of Brain Functions to Organization Response Elements

A key to moving out of the reptilian mode of response is through establishing the proper organizational structure/environment and the utilization of technology and automation. This will accomplish several things including removing the human from the area where he/she is most prone to react in a possibly erroneous manner by eliminating some level of confirmation bias. Additionally, this will enable the movement of higher-level functions to people and process. Ultimately this will lead to a highly effective organization that is resilient to the long-term impacts of trauma. In order to accomplish this, the organization must mimic the ability of the human system to survive. "Survival energies are organized in the brain and specifically expressed in patterned states of muscular tension in *readiness for action*." (Levine, 2010).

It is important to look at each area of the organizational response elements when crafting a strategy for the organization: **1) Automation 2) Process & Communication 3) Resilience & Learning.** While all these elements are critical and important and can be approached in parallel to some extent, automation is necessary to enable some of the higher level functioning.

8.1 Automation

The role of automation is critical in the phase of incident detection and analysis noted in the above incident handling process. The security industry is quickly coalescing around the criticality of this and numerous new categories such as security orchestration and automated incident response are emerging. It is a natural evolution of the security tools space as many teams struggle with an increasing volume and complexity of cyber events and a shortage of qualified incident responders. "The level of systemic complexity has increased to the point where manual response by security analysts is too difficult and ineffective." (Kindervag, John and Balaouras, Stephanie, 2014). Security tools and APIs have matured and there is increased opportunity to integrate external threat intelligence (IOCs, hash values, IPs) with internal information (logs, netflow data, malware samples). The realities of the threats and the solutions to address these complexities are further being fueled by a flood of venture capital money being directed at startups that are addressing this problem space.

Once the proper automation is in place it will allow humans to focus on the higher level processing and stay out of the reptilian response mode thus preventing any long term impacts of trauma.

8.2 Process and Communication

It is interesting that the elements of incident response that rely on people receive far less focus, time and energy than the technology. This is counter intuitive when you consider that humans orchestrate incident response and the development of humans should be at least as important as the development of technology.

When considering the process and communication area of response, it is important to look at alignment with the incident process of the larger organization, ensure understand and

training around the process and have a strong communication approach to at levels of the organization. Typically, most organizations have an incident response process for functions outside of security whether in their production operations or corporate IT function. It is important to integrate into those processes as much as possible when developing the security incident response process. Integration includes the severity rating nomenclature, the service level agreements (SLAs) for resolution, and the escalation process and procedure. Drawing the analogy to "physical health" being a key element for successful escape, there is a need to maximize resources to ensure the most effective response. This maximization comes through alignment of the processes and clarity on roles and responsibilities.

Relative to communication, it is important to have a predefined approach to communication. The communication plan should be well understood and people at all levels of the organizations should have had training on the plan. During the incident, it is critical to regularly update the predefined communication vehicles (emails, company website, employee intranet, etc.) and employees should be aware of these communication vehicles, how to access them and how to use them. It is recommended that if a bridge line is utilized for communication during an incident, that two different bridge lines are established one for the core incident team addressing the issue and a separate bridge line for executives. Having two different lines will help the core team perform their duties without the potential involvement of executives who have the tendency to try and solve the problem. Regular communication to the organization will build the trust of employees/executives and this will reduce the chance for longer-term traumatic effects to the organization.

During the time when there is not an active incident some kind of regular communication to employees educating them about breaches that occur outside of the company should be conducted. (Strand, John, 2015). This information will help employees understand that many companies are facing the challenge of breaches and helps educate them to the possibility, which in the end lessens the shock if it were actually to occur. Additionally, regular summary communications should go to the Board relative to incidents. This communication should include the summary of incidents and their severity, any impacts to the business or its operations and the actions being taken to improve the overall people, process and technology.

8.3 Resilience and Learning

Security teams operating in today's threat environment will at some point experience an attack. These attacks have the potential to cause enterprise wide trauma, as the author perceives would be the case for companies such as Target. Target experienced significant organizational trauma, which resulted in the dismissal of the CEO and CIO and derivative lawsuits against the Board and Officers. Because of the potential magnitude of this trauma, it is important to approach resilience and learning in a comprehensive and holistic manner involving all critical parts of the organization.

In the author's opinion, the incident response team should reach broader than just the technical teams and should include representatives from Customer Care, Marketing, HR, Legal, Public Relations, C-level Executives and the Board. Not all incidents will involve all these functions but it is important to have all functions trained and ready to respond if they are needed. Training of these functions is critical and the most effective way to accomplish that training is through incident response exercises.

There are several types of incident response exercises including tabletops, hybrid and full scales exercises. In a tabletop exercise, a paper-based scenario is scripted and the incident team is assembled in a meeting room of some type to run through the scenario and discuss how they would handle the situation. This is probably the lowest stress exercise as there are actually no real impacts to the environment. In a hybrid exercise, a paper based scenario is used in addition to a red team to simulate some level of real activity such as actually attempting to exploit a known vulnerability on an externally facing web site and the security operations center, aware of this attempt before the exercise starts, would respond. In full-scale exercises, the red team is given freedom to attempt to compromise the environment and a small group of people within the org is kept aware of the progress of the red team. In a full scale exercise people on the incident team don't know that this is only an exercise and obviously will this type of exercise will create the most stress in the organization. Regardless of the type of exercise conducted ensure that there is sufficient time to plan the exercise. Generally, a tabletop requires 1-2 months, a hybrid exercise takes 3-6 months and a full-scale exercise takes 6-12 months of planning. (Kick, Jason, 2014).

"It's only when you're faced with obstacles, stress, and other environmental threats that resilience, or the lack of it, emerge" (Konnikova, Maria, 2016). This points to the incredible

importance of incident response exercises, as they will promote an efficient and proper reflex response when an actual incident occurs. There are analogies to this within the human brain operation, "neuroplasticity, the relatively recent discovery that neurons that "fire together, wire together". When a circuit fires repeatedly, it can become a default setting—the response most likely to occur." (Van Der Kolk, 2014). As teams run various exercises, they build up their resilience and begin to fine-tune that response. This process builds the confidence of the team, ensures an escape route, and improves the communication. Most importantly, these elements allow the humans to think more clearly and stay out of the reptilian mode of response.

Another key to promoting resilience within a team is to turn a potentially traumatic event into an opportunity to learn. In order to avoid the long-term impacts of that attack, organizations must develop the resiliency and ability to learn post incident. "A central task for recovery from trauma is to learn to live with the memories of the past without being overwhelmed by them in the present" (Van Der Kolk, 2014). Obviously, a real attack is not perceived as a positive event at the time it is happening but the importance of spending a significant amount of time on lessons learned is critical and necessary to building a resilient team. With human trauma, "learning how to breathe calmly and remaining in a state of relative physical relaxation, even while accessing painful and horrifying memories, is an essential tool for recovery" (Van Der Kolk, 2014).

Just as humans tend to avoid reliving a traumatic event, organizations tend to avoid reviewing negative incidents. The author is of the opinion that this is one of the prime reasons for an incident team not pushing the importance of a lessons learned discussion. In order to build the proper resilience in the organization, a lessons learned session and associated follow up in action items is critical. Some important elements of conducting a lessons learned session include the following:

- Creating a safe environment
- Clear agenda and goals of the session
- Documentation of clear actions and owners

Relative to creating a safe environment this includes setting ground rules for the session, making it a relaxed environment (possibly consider taking the session outside of the normal office setting), possibly collecting anonymous feedback prior to the meeting ad probably most

importantly discussing what actually went right during the incident. During the meeting, staying focused on the actions and solutions versus placing blame will promote more open discussion and a broader participation.

8.4 Elements of Preventing Trauma in an Organization

In order to ensure that the organization can withstand the trauma of continuing cyber-attacks, there are specific steps to be taken. The table below summarizes the important elements to consider.

Incident Response Phase	Team Elements	Organizational Elements	Process Elements	Technology Elements
Preparation	• Trauma Training • Proper staffing • IR plan training	• **Incident response exercises** • Aligned IR processes • Training across organization • Promote conversation about incidents internally • Trauma training for Execs & Board	• Detailed response plan • Detailed communication plan • Retained firm to help with investigations/ forensics	• Current vulnerabilities • Current inventory of assets/owners • Intelligence program
Detection & Analysis	• Understanding technical strengths and limitations	• Consistent communication		• Automation
Containment, Eradication, and Recovery	• Rotation of staff to allow for rest	• Consistent communication		• Automation
Post Incident Recovery	• Address training gaps • Reassess staffing model	• Address communication plan gaps	• **Comprehensive Lessons Learned** • Follow up on action items	• Strong case management system • Address technology gaps

Table 1: Mapping of Incident Response Phase and Critical Elements of Response

The key to building the robustness of an organization around cyber-incidents is preparing the organization for the incident (training, exercises, communication, and repetition) and when it happens creating a learning environment where people are not penalized for the mistakes made

during the incident. If organizations fail to deal with the trauma, the reptilian mode of response will continue to be the prevalent response. Organizations will continue to be too scared to respond in a more sophisticated manner. They will continue to fail to resolve known security issues (denial), they will continue to handle breach communication improperly (avoidance), and as they fire those involved in the incident will prevent organizational learning (no escape and reinforcement of fear).

9. Conclusion

There are significant parallels between the impacts of trauma in individuals and the impacts of trauma in the form of cyber-attacks to organization. It is clear that there are valuable lessons learned from the extensive research that has been conducted relative to treating human trauma. It is imperative that we avoid having organizations move into a reptilian mode of response. This can be accomplished through improvements in Automation, Process & Communication, and Resilience & Learning. Automating the lower level data gathering and processing is critical to enabling the responders to move to a higher-level mode of processing and response. Relative to process and communication it is important to gain alignment around the incident process across the larger organization, ensure training around the process, and refine the communication channels and approach at all levels of the organization. In resilience and learning, all areas of the organization should participate in regular incident response exercises and lessons learned should emphasize and incorporated into the continuous improvement of the organizations response process. These elements of organizational trauma prevention are critical to the future of healthy response.

References

Lord, Nate. (2015). The History of Data Breaches. *Digital Guardian,* https://digitalguardian.com/blog/history-data-breaches

Cser, Andras, Ferrara, Ed, & Kindervag, John. (2015). Prioritize Tokenization to Secure the Payment Chain. *Forrester.*

SC Staff. (2015). Breaking news: EU agrees 4% fines for breaching data protection regulations. SC Magazine, http://www.scmagazineuk.com/breaking-news-eu-agrees-4-fines-for-breaching-data-protection-regulations/article/460046/

Van Der Kolk, Bessel. (2014). *The Body Keeps the Score*. New York: Viking Penguin.

Levine, Peter A. (2010). *In an Unspoken Voice*. Berkeley CA, North Atlantic Books.

National Center for PTSD, Symptoms of PTSD. (2015) *US Department of Veteran Affairs,* http://www.ptsd.va.gov/public/PTSD-overview/basics/symptoms_of_ptsd.asp

Creswell, Julie & Perlroth, Nicole. (2014) Ex-Employees Say Home Depot Left Data Vulnerable. *The New York Times*, http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html

Schwietzer, Sonja & Pross, Christian. (2010). The Culture of Organizations Dealing with Trauma: Sources of Work-Related Stress and Conflict. *Traumatology* 1 6(4) 97-108.

Woods, Bob. (2016). Virtual extortion is big business for cyber criminals. *The Hacking Economy, CNBC, http://www.cnbc.com/2016/02/17/ransomware-is-targeting-us-companies-of-all-sizes.html*

Constantin, Lucian. (2016). Jigsaw crypto-ransomware deletes more files the longer you delay paying. *CIO magazine*, http://www.cio.com/article/3054735/jigsaw-crypto-ransomware-deletes-more-files-the-longer-you-delay-paying.html

SANS Security 401 Security Essentials Bootcamp Style. (2015). *Defense in Depth, 401.2*.

Cichonski, Paul, Miller, Tom, Grance, Tim, & Scarfone, Karen. (2012). *Computer Security Incident Handling Guide.* National Institute of Standards and Technology Special Publication 800-61 Revision 2.

Ranum, Marcus (2015). Challenging Your Incident Response Process. *IANS AAE Answer*.

Kindervag, John & Balaouras, Stephanie. (2014). Rules of Engagement: A Call to Action to Automate Breach Response. *Forrester.*

Strand, John (2015). Incident Response Internal Communication Best Practices. *IANS AAE Answer.*

Kick, Jason. (2014). Cyber Exercise Playbook. *The MITRE Corporation.*

Konnikova, Maria. (2016). How People Learn to Become Resilient. *The New Yorker*, http://www.newyorker.com/science/maria-konnikova/the-secret-formula-for-resilience

Rittenghouse, John W., & Hancock, William M. (2003). *Cybersecurity Operations Handbook.* San Francisco, Elsevier Digital Press.

Ponemon, Larry. (2014). Ponemon Institute Releases 2014 Cost of Data Breach Study: Global Analysis. *Ponemon Institute*, (http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis)

Balaouras, Stephanie, Shey, Heidi, Iannopollo, Enza & Holland, Rick. (2015) Lessons Learned From the World's Biggest Customer Data Breaches and Privacy Incidents 2015. *Forrester*.