Threat Rigidity in Cybersecurity

Mike Weeks

Threat Rigidity in Cybersecurity

GIAC (GCCC) Gold Certification

Author: Michael Weeks, mweeks9989@gmail.com
Advisor: Stephen Northcutt
Accepted: October 25, 2017

Template Version September 2014

Abstract

Fear Uncertainty and Doubt (FUD) works as an influence strategy by amateur cybersecurity professionals over an organization, and as a result, FUD Fatigue develops causing a negative impact on their credibility (Anderson 2014). Is there a better way to effect change while maintaining credibility? A social science theory called Threat Rigidity (Staw et al.,1980) addresses organizational responses to threats by describing a constriction in control and a restriction in information processing. The theory of Threat Rigidity theory and its concepts describes FUD Fatigue in that FUD is utilized to spur the threat-rigidity response and will cause a decrement in performance when the level of response is inappropriate for the threat. Threat Rigidity leveraged by a competent cybersecurity professional allows for not only the management of a threat but also the ability to implement critical controls to safeguard the organization from future attacks and move the organization back into an innovative state.

1. Introduction

Early in a security professional's career, the security issue seems exceptionally daunting. Coupled with the newly gained knowledge of all the different attacks that competent attackers can utilize and the vulnerabilities that already exist, it is easy to see how a novice may be quick to escalate any security issue to a high level. Sounding the alarm a few too many times for a low-risk vulnerability or security issue, especially with an agenda, will ensure that a security professional loses credibility for himself and his department. Even worse is suggesting a solution that is not applicable to the perceived risk. The utilization of Fear, Uncertainty, and Doubt (FUD) to push an agenda will quickly exhaust all political capital and credibility a security practitioner has with his organization (Anderson 2014). Also, if a cybersecurity professional squanders resources on an inappropriate response to a perceived threat, then the organization will move further into Threat Rigidity causing further harm to the group.

There are multiple places where one can learn how to respond to threats appropriately. One excellent source for prioritization information would be the Critical Controls from the Center for Internet Security. When deciding what projects to address having an independent competent assessment based on real-world offensive actions is indispensable. SEC 566 gives an in-depth breakdown of how to prioritize security controls and whether to spend time and energy on a security initiative. However, research on messaging and its effect on cybersecurity projects appear to be limited.

According to the theory of Threat Rigidity, there will be a constriction in control in response to a threat. Enhanced control by leadership is the main reason that FUD works to motivate an organization to change. The Security Practitioner is given authority due to his or her perceived competence in the instance of a cybersecurity threat; and, according to the same theory, information processing will restrict central cues and prior expectations (Bakk 2007). In response to the regression of information processing, careful and guarded messaging by a cybersecurity professional should communicate they are responding to the threat with a valid mitigation.

Does the theory of Threat Rigidity affect cybersecurity? Determining this will require an analysis of Threat Rigidity. One way is to ascertain if high-profile threats result in successful cybersecurity initiatives, and if messaging is critical to the success of those security projects and the continued credibility of the cybersecurity professional.

Michael Weeks, mweeks9989@gmail.com

Highly visible cybersecurity events likely have the effect of moving organizations into a Threat Rigidity state, and many seasoned cybersecurity professionals utilized these events to fast-track a current or planned cybersecurity initiatives. How cybersecurity personnel leveraged these events and the role messaging applied is a core research goal for this paper. Whether security practitioners utilized current known threats to ensure projects meet future threats is also a research question. These high-visibility events offer the opportunity to study how perceived threats could affect an organization.

2. Threat Rigidity

When an organization experiences a crisis, it will focus on its core competency and become more rigid in the hierarchical in its organization. An effect called Threat Rigidity which also has the result of stifling innovation into new competencies. Mitigating the risk of the threat and potential new threats will assist an organization to move out of this state and back into an innovative state. Information Security threats have grown to threaten the existence of companies and potentially drive organizations deeper into Threat Rigidity. A significant role of the cybersecurity professional is to mitigate cybersecurity risks, so organizations feel safe enough to move into an innovative and trail-blazing organization.

Information Security applies mostly to organizational threat rigidity however, to understand threat rigidity in organizations it is important to understand its roots, in Biology. In Biology, the stress chemical cortisol floods the body elevating the heart rate and increases adrenaline production (Dickerson 2004). The process is part of the Fight or Flight Response. One significant aspect of the Fight or Flight Response is the hindrance in the growth of tissue, and in some extreme cases organs will shut down. When an individual is under a perceived threat, the system unifies to respond to the threat by focusing critical systems and energy to react until the is over.

Leaders who don't understand cybersecurity threats engage the same primitive system when trying to deal with the threat. The newest attack could trigger the same Flight or Fight Response as a deer being chased by a pack of wolves. The deer is not worried about growing hair, mating, or digesting whatever it has eaten recently. It is concerned about running as fast as possible to get away. After the deer can get away, the cortisol levels reduce, and the deer can get back to growing, eating, and making more deer. This is the same effect of a perceived

existential threat against an organization based on a cybersecurity threat that they do not comprehend. Leadership will become rigid in its operations and focus on what the organizational core competency until the threat is alleviated. Rigid operations will lead to a stagnant existence which will prevent growth and innovation, the same way an animal does not grow when running from a predator.

During a Flight or Fight Response, the hormone Cortisol spikes in the individual. In groups, the Cortisol response can be detected by others in a group and causes the same stress response to occur in other individuals near to the first member of the group to initiate the cortisol stress response in others. This shared fear-response is an evolutionary adaption that social animals have developed to ensure that all members of the group are aware of the danger as soon as possible and all have an equal opportunity to escape the threat. Shared cortisol response is a critical survival response for social animals, and that humans are the most complicated social animal there is.

Organizational Threat Rigidity describes the same effect as a shared cortisol response but on a much larger scale and with much more complex animals. The group will direct all resources available to deal with an aggressor. Responses to attackers can result in the restriction of information processing or a constriction in the control of the organization (Kamphius 2008). Cybersecurity Professionals provide leadership to the group as the perceived expert in the field and receive the temporary constriction of control vicariously. Messaging around the threat could easily rely on fear, uncertainty, and doubt where the cybersecurity professional touts shadowy undefined attackers with a response that barely fits the aggressor. However, the better reaction is clear and concise messaging regarding the actual risk based on preconceived notions and expectations with a central cue from a dominant response (Kampius 2008).

A cybersecurity practitioner could utilize the effects of threat rigidity by leveraging a perceived cybersecurity threat to fast-track a security initiative which should mitigate the perceived attacker and move the organization into a more productive posture. Ensuring the legitimacy of the response is of the most importance. These corrective actions will likely pull from other activities that an organization needs for growth. If the initiative is perceived to be valid, then responding to the threat by restricting some resources for growth and innovation is valid. If the messaging around the reaction does not outline the validity of the response, then an initiative will fail, and the security practitioner will lose credibility.

Michael Weeks, mweeks9989@gmail.com

Leaders and individuals perceive cyberattacks to the organization and call upon cybersecurity personnel to address threats. It is not enough for a cybersecurity professional to respond, he must ensure that the communicated response conveys the problem in a clear and concise manner to ensure the perceived validity of the reaction. Threat Rigidity theory compounds this challenge in that organizations will rely on preconceived information that has worked in the past. When a newer type of threat such as an emerging cybersecurity attack faces a group, then the organization could move into a state of Threat Rigidity and its ability to adapt to the change will be hampered without expertise in the subject matter and the ability to properly communicate that expertise.

With the concept of Threat Rigidity in mind, a cybersecurity professional can adapt his messaging to consider preconceived beliefs and hypothesis when developing a messaging strategy. Understanding the culture and history of an organization must be cataloged along with any past incidents to determine if they are applicable in the current situation. According to the theory, past successful strategies will be much easier to implement during a crisis. However, the difference between FUD and a successful implementation is an appropriate response coupled with controlled messaging.

3. High Profile Threat Events

Over the recent months, a few high- profile cybersecurity attacks reported by the national media highlighted cybersecurity attacks and vulnerabilities. WannaCry, a ransomware that resulted from an exploit-kit released by the mysterious shadowbrokers group, was a self-replicating worm that became a terror to the internet early in Summer 2017 (Woolaston 2017). Petya, another ransomware, was successful where WannaCry was not. Petya used the same exploits but paired it with phishing attacks.

Each of the previously described high-visibility events could have been mitigated using very few security initiatives. Applying MS17-010, a patch that came out 2-3 weeks before WannaCry could have reduced its attack surface before its release. Also, at the time of this paper, there is no indication that WannaCry spread through phishing, which means that it scans and exploits port 445 on the IPv4 public network. Almost all border firewalls block TCP port 445 inbound and most block at the network egress points and would have easily prevented this attack. Fortunately, WannaCry had significant press attention, and a cybersecurity practitioner could

have taken advantage of the situation to inform leadership on the benefits of expedited patching and firewall segmentation which is a valid response to the perceived threat.

Petya, considered "WannaCry 2.0", where the attacker glued phishing attacks as well as WMIC attacks and the MS17-010 attack to spread as much as possible. Communicating this through proper messaging to leadership and the rest of the company allows for the opportunity for security initiatives such as email security, malware controls, increasing patch frequency, or Active Directory hardening. Multiple

4. Research

4.1. Research and Survey Questions and Methodology

How does an organization verify that threat management, crisis management, and security initiatives balance with the organization to support the group as opposed to stealing away resources without mitigating the risk? Messaging is critical to the handling of a threat in a manner that will ensure credibility regardless of the response (Schmidt 2016). The other aspect of a successful security initiative is for the project lead to be skilled and knowledgeable in the cybersecurity profession. The response to the perceived threat must be correct and proportional combined with messaging to ensure that management and the organization are aware of the reasoning of the action/reaction.

Does Threat Rigidity theory apply to cybersecurity? Testing and evaluating this research question will utilize survey methodology, open-ended questionnaires, and direct interviews. Determining messaging content is difficult to ascertain with a standard closed question survey. Understanding what competent cybersecurity professionals used as communication to management and the organization is critical to understanding how to manage expectations in response to a crisis. One method is to have an open-ended discussion with the advisory board through the SANS organization. The answers provided by this list occupied by some of the elite of cybersecurity professionals should provide examples of competent messaging examples.

A general list of questions sent to some to the cybersecurity community will determine the effects of high-visibility events and the importance of messaging around the proposed mitigation. This is a direct questionnaire asking: "did a security initiative result from WannaCry and was messaging important?" Results are categorized by each question and graphed in section 4.2 Findings.

An open-ended request was sent to the SANS advisory board regarding their messaging in response to high-visibility events. Eight security professionals responded with detailed information regarding the research. A questionnaire sent to 550 cybersecurity professionals of which 21 recipients completed the survey ranged from security engineers and analysts to managers and CISOs. High-visibility threats correlated with the ability to accomplish security initiatives, and a positive correlation between messaging and successfully implementing a security initiative showing support for the hypothesis.

Unfortunately, the prior two methods only capture the input from cybersecurity professionals. While critical to this research, it does not answer all the questions purposed. Whether there is a gain or loss in credibility, the perception of the security team's efficacy and relationship to the security team needs to be measured. Gartner, according to their website, "is the worlds' leading research and advisory company" (Gartner 2017). One of the biggest conferences is the Gartner Symposium/ITxpo 1-5 October 2017, Orlando, FL and also according to Gartner, "one of the most of the world's most important gathering of CIOs and Senior IT Executives" (Gartner 2017). Interviewing Senior-Level IT executives provides the level of feedback needed to answer the question: have cybersecurity teams lost or gained credibility after successfully deploying a security change in response to a high-visibility threat?

4.2. Findings:

Interviews conducted with 38 different self-identified Senior level IT and CIOs at the Gartner ITXPO provided insights into the perception of cybersecurity personnel. Without being prompted, interview subjects highlighted the high-importance of cybersecurity in technology today. Multiple CIO/IT respondents rated the performance of the security team higher dependent upon whether the security team was a subordinate to IT or in a separate organization. Respondents who did not know if security teams responded to high-visibility events (21%) rated the response to security events more poorly. The poor perception of security teams based on their visibility is supportive of the idea that messaging, and communication is critical to ensuring the organization perceives a valid response to the threat.

The second survey restricted to a 1-5 scale-based answer distributed via social media. Twenty of the twenty-one survey takers had positive remarks regarding high visibility events fast-tracking security initiatives. Messaging was also found to be favorable to successful security

projects after a cyber-security threat dominates the news cycle. Also, a slightly higher percentage of respondents highlighted messaging to management rather than messaging to employees.

4.2.1. Questionnaire to advisory board

Seven out of the eight respondents stated that they utilized the high visibility events to fast-track security projects. One respondent who did not utilize the increased visibility to focus on an initiative did use the emergency to bump some of the projects that were months or years behind. This critical evaluation of prioritized projects in the management of an organization takes courage and is an excellent option for a response-based action. Initiatives that could be fast-tracked were application white-listing, removal of administrative rights and patch management.

Every respondent but one stated they used email for communication. All were adamant that they used learning events with activity booths and a corporate intranet website. Another respondent spoke highly of a bi-weekly newsletter to executives focused on current high visibility events and how the security team is responding to those events. The communication was top-down primarily utilizing a security executive.

All respondents stated they did work heavily on communication with management – however, the methods did differ. Some sent newsletters, some weekly conference calls, and some did in meetings or briefings. As a result, some professionals utilized intel reports or developed a process to provide intelligence reports to senior management. The theme around the responses is that communication to management occurred frequently and thoroughly.

According to the respondents, messaging concerning the incidents was varied. Some respondents focused on the event, some around the response, and some around threat management. One fascinating account was regarding messaging around a compromise from WannaCry. The company had been impacted by WannaCry and controlling the information from a public relations perspective through proper messaging was critical. Some of the safeguards that taken were, no written communication and in-person only meetings as well as voice-only phone calls and no emails concerning/regarding the incident.

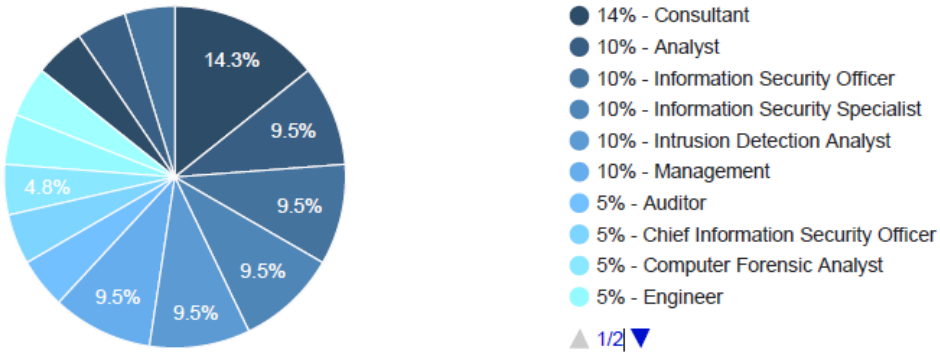
Respondents were adamant that they had internal communication in the incident response procedures, however three respondents realized that they needed to update them to fully integrate messaging into their crisis management and incident response plans.

4.2.2. Questionnaire to security professionals

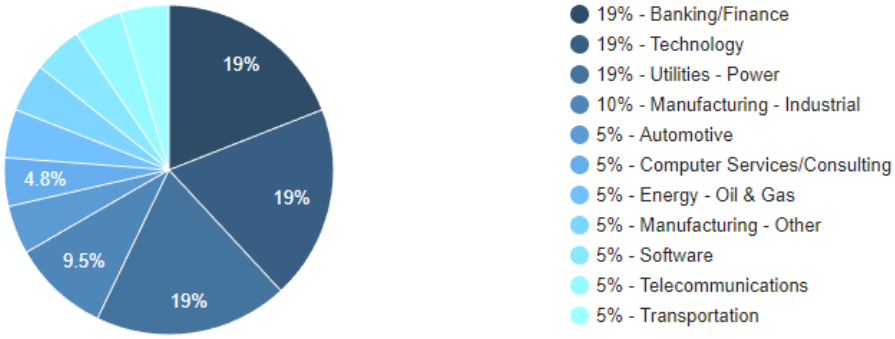
No technology rose to the top, in fact, two respondents stated that technology was not the solution to their problem. Increasing patch frequency, however, was the initiative that was focused on the most. The following section provides the specific breakdown of answers to the survey questionnaire.

4.2.3. Answers to Questionnaire:

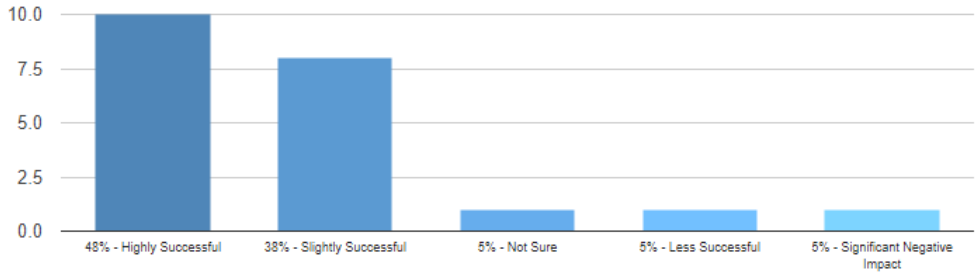
1. Which of the following best describes your role? (regardless of job title)



2. In which organization/industry is your employer?



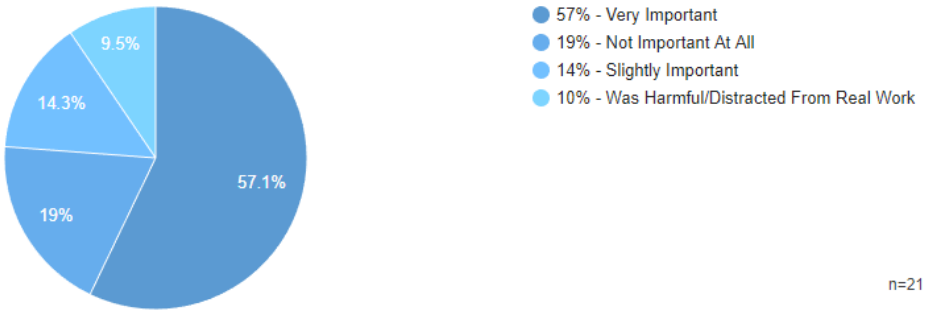
3. How successful have you been able to leverage high visibility events to fast-track security initiatives?



4. How much did the crisis improve/impact the timeline of the deployment of your security project?

Response	Total	% of responses	%
Significantly Improved	9		43%
Slightly Improved	8		38%
Slight Negative Impact	2		10%
No Impact	2		10%
Significant Negative Impact	0		0%

6. How important was controlling the messaging to the company?



Michael Weeks, mweeks9989@gmail.com

7. What type of security initiative did you prioritize as a result of the perceived security threat?

Response	Total	% of responses	%
Other, please specify	6		29%
Increasing Patch Frequency	6		29%
System Hardening	4		19%
Inventory of Devices	2		10%
Application White-Listing	2		10%
Inventory of Software	1		5%
	Total respondents: 21 Skipped question: 0	0% 20% 40% 60% 80%	

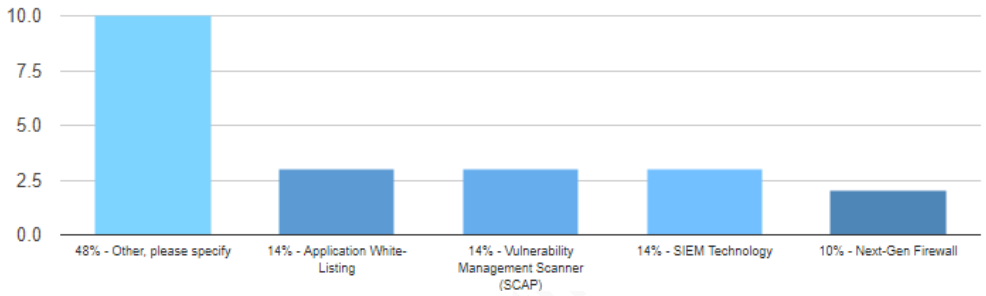
Respondents also could respond with - “Other, please specify” – the following were all specified by individual respondents.

Response
interrupted an important audit which is security
n/a
All of the above, but ONLY after a comprehensive Red Team Engagement owned they infrastructures.
Update it remove 3rd party software
Ship new detection content
Supply chain security planning

Showing 1 to 6 of 6 rows

Michael Weeks, mweeks9989@gmail.com

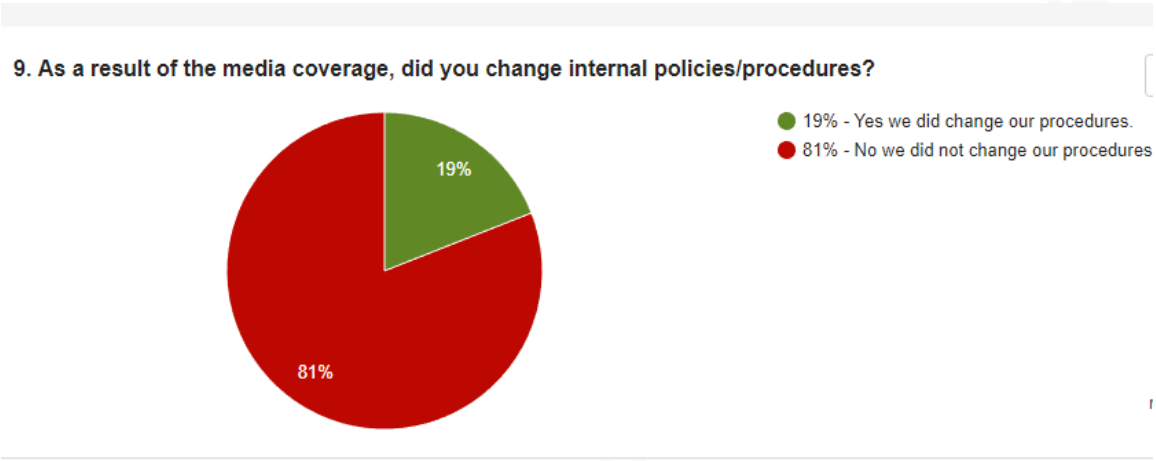
8. Did you look at purchasing a new security technology?



Respondents could also select – "Other, please specify" – with the following results:

Response	Responded
no	Last Tuesday at 9:43 AM
SCCM	Last Tuesday at 9:19 AM
No. Technology isn't the answer.	08/06/2017
SDN	08/06/2017
No	08/05/2017
No	08/04/2017
None	08/03/2017
No new tech, just better utilization of existing.	08/03/2017
Network segmentation	08/03/2017
HIPS	08/03/2017

Michael Weeks, mweeks9989@gmail.com



4.2.4. CIO and IT Management Interviews and Responses:

A strong positive correlation between whether the security team is organizationally subordinate to the CIO and how the CIO rated the security team's response to high-visibility events. While 68% of respondents stated they would trust the security team to handle future high-visibility events, all CIOs said that they would not if the security team were not a subordinate organization. Respondents scored the security team's response more positively if they were a peer group as opposed to being separate.

The response rating regarding how security teams handled high-visibility events was also proportional to whether there was a perceived response to the incident.

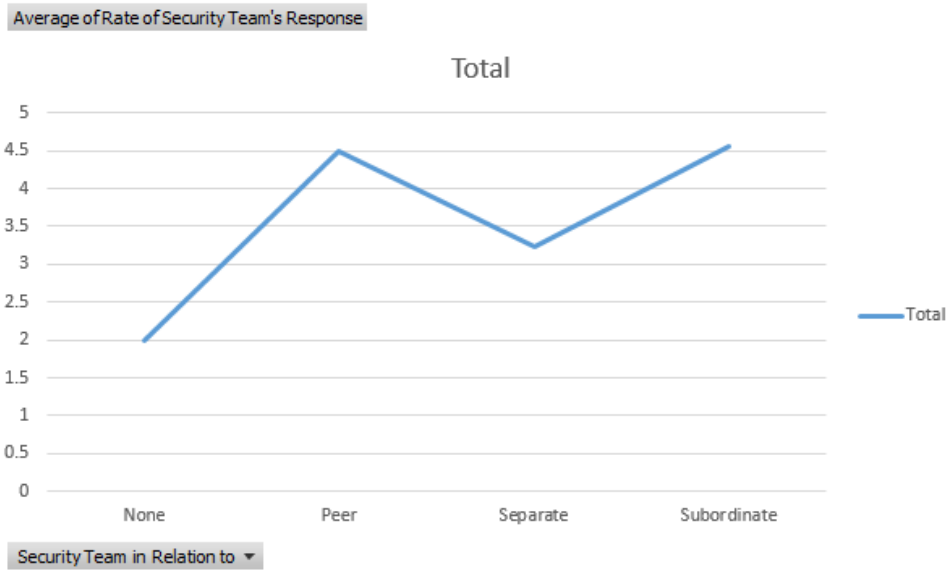
Figure 1: Types of Responses

Location of Security Team Related to CIO	Average Rate of Security Team's Response High-Visibility Events
Separate	1.666666667
Subordinate	4.5

Row Labels	Count of Role
Application Developer Architect	1
Architecture Management	1
Artificial Intelligence Engineer	1

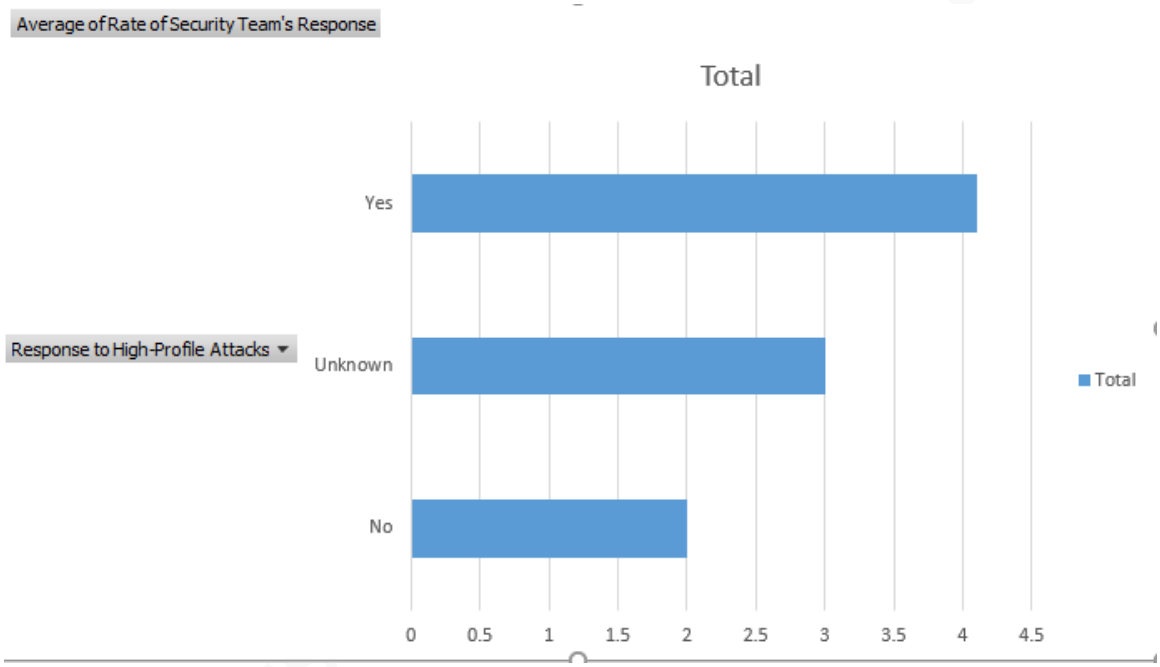
Michael Weeks, mweeks9989@gmail.com

CIO	5
Data Analytics Manager	1
Database Management	1
Developer	1
Digital Transformation Architect	1
Digital Transformation Researcher	1
Enterprise Architect	2
IOT Director	1
IT Director	3
IT Manager	3
IT Planner	1
IT Strategist	1
Lead Developer	1
Network Manager	1
Product Manager	1
Project Manager	1
Researcher	1
Sales	1
Sales Engineer	2
Sales Manager	1
Sales Representative	2
Senior Application Architect	1
System Engineering Manager	1
Windows Manager	1
Grand Total	**38**

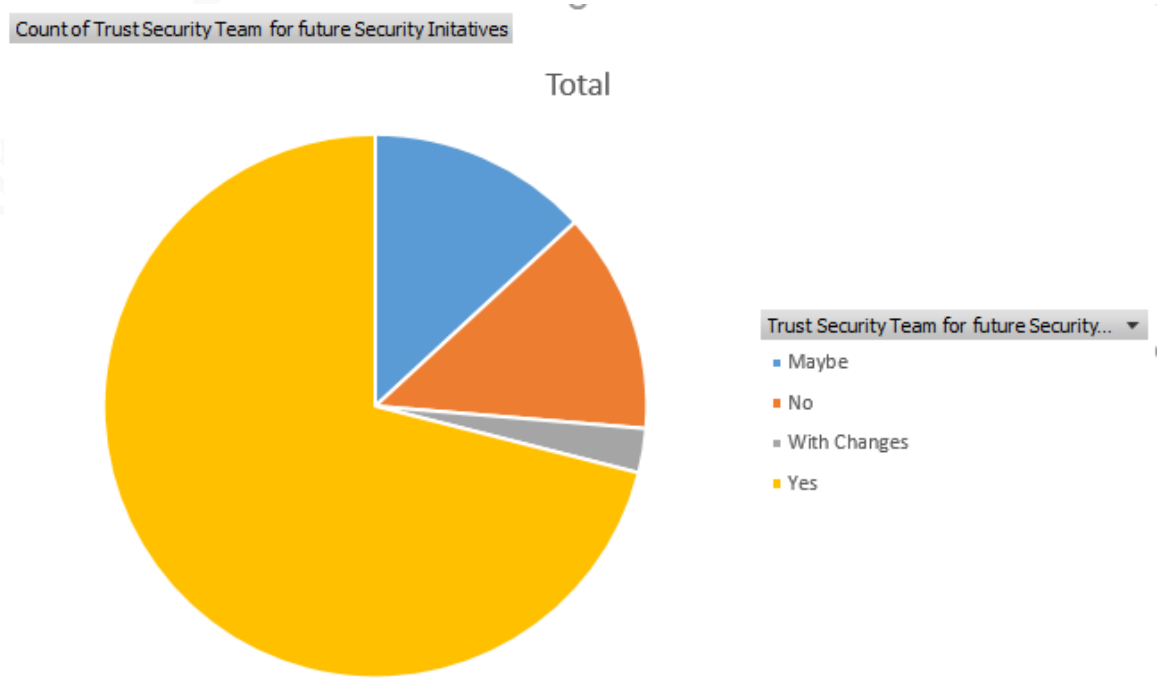


Michael Weeks, mweeks9989@gmail.com

The hierarchical location of the security team in relation to IT and how they are rated is the first graph.



Percentage of survey takers who are aware if security team responded recent events, and if they responded to the events.



Michael Weeks, mweeks9989@gmail.com

5. Conclusion

Survey results from cybersecurity professionals confirmed high-visibility events assisted them in fast-tracking security actions. Also, a high number of sampled cyber professionals assigned a high rating to "messaging" and its effect on successful security projects. Threat Rigidity theory appears to apply to cybersecurity, and security professionals should heed some of the aspects of this hypothesis. When an organization perceives a threat to its existence, the group will respond using the concepts in Threat Rigidity theory in response to the threat. There is a constriction in control where leadership will focus resources on dealing with the threat. Also, there is a restriction of information with a focus on preconceived notions and hypothesis. Messaging must encompass the culture of the environment and past incidents to ensure that the security initiative is fast-tracked. A successful Cybersecurity professional will mitigate the threat with a successful response, ensure the response is communicated to the organization, and assist the organization move from a Threat Rigidity state and into an innovative state.

According to responses, the answer does not lie in any individual technology or process. However, implementation of the critical controls such as patching, or application whitelisting were highly praised. These security initiatives continue to be invaluable to defend against new and advanced threats.

Guiding an organization through a change in response to an existential threat is not a trivial skill. This ability is something that cybersecurity professionals must attain to be successful. Ensuring an organization is confident that a cybersecurity professional is managing a response is arguably just as important, if not more so, than implementing a technical control. During times of crisis, a security professional has a small window to fast-track an initiative. However, proper messaging is required to ensure that a cybersecurity professional can maintain his or her credibility.

Messaging in-line with the theory of Threat Rigidity consists of managing prior experiences and hypothesis while attempting to convey a new idea in response to a threat. Any message to a group must contain the minimal amount of information necessary to provide critical info to support the reaction to a threat. Not only evaluating all data points, messaging also carefully considers how the recipient perceived those data points. Knowing an audience and what preconceived ideas and hypothesis they may bring is central to proper communication, especially in a threat-response scenario.

Michael Weeks, mweeks9989@gmail.com

In the end, cybersecurity professionals have the choice of dealing with a current issue in a way that will either agree or disagree with the organization. Political capital should be a factor when responding to a threat. Falling too out of line with the group may result in a political toll that could be almost unsalvageable. With the continued loss of credibility, the security team will erode the justification of its existence in an organization. Cybersecurity professionals would do well to learn to ensure that all responses are adequate, within reason to the threat and that the reaction is communicated carefully with a controlled message to superiors and the rest of the organization. In doing this, the cybersecurity team can show immense value to an organization by enabling trust, safety, and security to encourage organizations to move from an organization operating in Threat Rigidity to an innovative organization with growth potential.

Michael Weeks, mweeks9989@gmail.com

References

Anderson, Kerry A. (2014), *The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture.* ISBN: 148220075,9781482220070, Publisher: CRC Press 2014, P.12-15, from https://books.google.com/books?id=tZt_AwAAQBAJ&pg=PA12&lpg=PA12&dq=FUD+impact+on+credibility+of+cyber+security+professionals&source=bl&ots=lQVoP2_3WA&sig=QPr7MSenquu-1XD06EHrF97t2_w&hl=en&sa=X&ved=0ahUKEwjK34CO1KzWAhVi4IMKHc2LAQoQ6AEIKDAA#v=onepage&q=FUD%20impact%20on%20credibility%20of%20cyber%20security%20professionals&f=false

Bakk, Mag, Manfred Hammerl. (2007). *Threat-Rigidity Hypothesis, An analysis of six scientific papers.* The University of Graz; Retrieved August 14, 2017, from http://www.grin.com/en/e-book/94346/threat-rigidity-hypothesis.

Dickerson, S. S., & Kemeny, M. E. (2004). *Acute Stressors and Cortisol Responses: A Theoretical Integration and Synthesis of Laboratory Research*. Psychological Bulletin, 130(3), 355-391. http://dx.doi.org/10.1037/0033-2909.130.3.355

Fox-Wolfgramm, Susan J.; Boal, Kimberly B.; Hunt, James G.: *Organizational Adaption to Institutional Change: A Comparative Study of First-order Change in Prospector and Defender Banks, in Administrative Science Quarterly*, Vol. 43, 1998, p. 87-126

Holm, Peter. *The Dynamics of Institutionalization: Transformation Processes in Norwegian Fisheries, in Administrative Sciences Quarterly*, Vol. 40, 1995, p. 398-422

Kamphius, Wim; Gaillard, Anthony (2008), *Threat-Rigidity Effects on Planning and Decision Making in Teams*, Netherlands Defence Academy, Breda, The Northlands

Newman, Karen L.: *Organizational Transformation during Institutional Upheaval, in Academy of Management Review*, Vol. 25, 2000, p. 602-619

Quinn, James Brian (1980). *Managing Strategic Change;* MIT Sloan. Retrieved August 14, 2017, from http://sloanreview.mit.edu/article/managing-strategic-change. Quinn, James Brian

Schmidt, Allison M; Ranney, Leah M.; Pepper, Jessica K.; Goldstein, Adam O. *Tobacco Regulatory Science, Number 1*, January 2016, PP 31-37(7): Tobacco Regulatory Science Group: Https://doi.org/10.18001/TRS.2.1.3

Michae

Staw, Barry; Sandelands, Lance E.; Jane E. Dutton (1981). *Threat Rigidity Effects in Organizational Behavior: A Multilevel Analysis.* Retrieved August 14, 2017, from http://webuser.bus.umich.edu/lsandel/PDFs/Threat%20Rigidity%20Effects.pdf.

Woods, Laura (2017). *The 4 Phases of Crisis Management.* Chron. Retrieved August 14, 2017, from http://smallbusiness.chron.com/4-phases-crisis-management-77610.html.

Woolaston, Victoria (2017); *Wannacry ransomware: What is it and how to protect yourself, The latest on the MS17-010 flaw and the WannaCry patch linked to the NHS Cyber Attack*; Wired Magazine; http://www.wired.co.uk/article/wannacry-ransomware-virus-patch

Michael Weeks, mweeks9989@gmail.com

Appendix A - Questions to the SANS Advisory Board

Questions:

1. During the WannaCry, Petya or other high visibility events were you able to utilize the event to fast-track security initiative(s)?

2. Did you use any of the following methods for communication? Lunch and learns, email, top-down communication, etc.

3. Did you communicate to management around the situation?

4. What was your messaging around the event?

5. Have you added internal communication and messaging to your procedures in the future?

Michael Weeks, mweeks9989@gmail.com

Appendix B – Automated Survey Results

Which of following best describes your role? (regardless of job title)

1. In which organization/industry is your employer?
2. How successful have been able to leverage high visibility event to fast-track initiatives?
3. How much did the crisis improve/impact the timeline of the deployment of your security project?
4. How important was controlling the messaging to management?
5. How important was controlling the messaging to the company?
6. What type of security initiative did you prioritize as a result of the perceived security threat?
7. Did you look at purchasing a new security technology?
8. As a result of the media coverage, did you change internal policies/procedures?

Michael Weeks, mweeks9989@gmail.com

Appendix C – Questionnaire to IT and CIO personnel

1. What is your role in your organization?
2. Where is the Security team located in your organization?
3. Has your security team responded to the recent high-profile attacks (such as wannacry, Petya, not-petya, Equifax etc) by suggesting or implementing change?
4. How would you rate your security team's response?
5. Has the changes or initiatives your security team recommended been successful?
6. Would you trust your security team to make recommendations for security initiatives in the future?

Michael Weeks, mweeks9989@gmail.com

Last Updated: April 24th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Bucharest May 2019	Bucharest, RO	May 06, 2019 - May 11, 2019	Live Event
SANS Security West 2019	San Diego, CAUS	May 09, 2019 - May 16, 2019	Live Event
SANS Perth 2019	Perth, AU	May 13, 2019 - May 18, 2019	Live Event
SANS Stockholm May 2019	Stockholm, SE	May 13, 2019 - May 18, 2019	Live Event
SANS Dublin May 2019	Dublin, IE	May 13, 2019 - May 18, 2019	Live Event
SANS Milan May 2019	Milan, IT	May 13, 2019 - May 18, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VAUS	May 19, 2019 - May 24, 2019	Live Event
SANS New Orleans 2019	New Orleans, LAUS	May 19, 2019 - May 24, 2019	Live Event
SANS Autumn Sydney 2019	Sydney, AU	May 20, 2019 - May 25, 2019	Live Event
SANS MGT516 Beta Two 2019	San Francisco, CAUS	May 20, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, NL	May 20, 2019 - May 25, 2019	Live Event
SANS Hong Kong 2019	Hong Kong, HK	May 20, 2019 - May 25, 2019	Live Event
SANS Krakow May 2019	Krakow, PL	May 27, 2019 - Jun 01, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
Enterprise Defense Summit & Training 2019	Redondo Beach, CAUS	Jun 03, 2019 - Jun 10, 2019	Live Event
SANS London June 2019	London, GB	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS Zurich June 2019	Zurich, CH	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS Kansas City 2019	Kansas City, MOUS	Jun 10, 2019 - Jun 15, 2019	Live Event
SANS SEC440 Oslo June 2019	Oslo, NO	Jun 11, 2019 - Jun 12, 2019	Live Event
SANSFIRE 2019	Washington, DCUS	Jun 15, 2019 - Jun 22, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LAUS	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Cyber Defence Canberra 2019	Canberra, AU	Jun 24, 2019 - Jul 13, 2019	Live Event
SANS ICS Europe 2019	Munich, DE	Jun 24, 2019 - Jun 29, 2019	Live Event
SANS Paris July 2019	Paris, FR	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Cyber Defence Japan 2019	Tokyo, JP	Jul 01, 2019 - Jul 13, 2019	Live Event
SANS Munich July 2019	Munich, DE	Jul 01, 2019 - Jul 06, 2019	Live Event
SEC450 Security Ops-Analysis Beta 1	Crystal City, VAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Charlotte 2019	Charlotte, NCUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Muscat April 2019	OnlineOM	Apr 27, 2019 - May 02, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced