Ethical Dilemmas for Young Security Professionals in Corporate America

This abbreviated case study was compiled from published government and media sources, and is intended to be used as a basis for classroom discussion rather than to illustrate either effective or ineffective handling of a security leadership situation.

Preface

The purpose in publishing this case study is not to ridicule those involved.

In fact, most people reading this, if they were in a similar position as those 20-somethings named in this case, would have obeyed orders and stood trial too — and if you believe otherwise, then you're no student of history or psychology.

In my humble opinion, this case that follows is one of the single most important corporate security stories that any young professional can read. It's a horror story about how young professionals are susceptible to being led astray one step at a time by authority figures in their organization, from cyber stalking behaviors to deceiving law enforcement investigators.

Ethical Dilemmas for Young Security Professionals in Corporate America

Background and Initial Planning

The incident's genesis was rooted in the perception by senior [Company] employees that an online newsletter's critical coverage posed a reputational threat. In response, [Company]'s Senior Director, along with the Senior Manager, and other personnel, covertly planned a harassment campaign against the newsletter's editor (Victim 1) and publisher (Victim 2), who were a married couple residing in Massachusetts. The security team's preparations for harassment, which commenced in early August 2019, involved the creation of quasi-anonymous Twitter accounts aimed at sending threatening and disparaging messages to Victim 1, along with plotting physical surveillance and disturbing home deliveries to unnerve the victims.

Initiation of the Cyberstalking Campaign

By mid-August 2019, the cyberstalking phase was in full swing, although they never referred to it internally that way according to published reports. The security team used fake Twitter accounts to send a barrage of intimidating messages to Victim 1, including personal insults and explicit threats. Notably, they publicly posted the victims' home address, a tactic known as doxing. Concurrently, the team orchestrated a series of alarming deliveries to the victims' residence, including a bloody pig Halloween mask, live insects, and a book on grieving the loss of a spouse, all under the guise of anonymity using prepaid debit cards and fake online accounts.

Escalation and Physical Surveillance

The harassment intensified with further deliveries, such as a funeral wreath and pornographic magazines, addressed in Victim 2's name to their neighbors, aiming to embarrass and isolate the victims in their community. Sr. Director, along with Director and other [Company] personnel, conducted covert surveillance in Natick, MA. They followed Victim 2 and even considered breaking into the victims' garage to place a GPS tracker on their car. The victims reported these incidents to the Natick Police Department (NPD), which began an investigation and eventually linked some activities back to [Company] employees.

Police Investigation and [Company]'s Internal Panic

Upon learning of the NPD's investigation, the [Company] team launched a series of actions to obstruct the investigation, preparing false narratives and misleading documents for potential meetings with the NPD. Manager, posing as an [Company] representative, implemented a "White Knight Strategy" by contacting the victims and falsely offering [Company]'s assistance against the harassment. To cover their involvement, the conspirators deleted incriminating communications and data from their electronic devices.

Investigation Escalates and [Company] Responds

The FBI's intervention led to the unsealing of criminal complaints and charges against the involved [Company] employees, including conspiracy to commit cyberstalking and witness tampering. [Company] responded by conducting an internal investigation, which resulted in the administrative leave and subsequent termination of Sr. Director, Director, Sr. Manager, and other involved employees. The case revealed significant ethical breaches and illegal activities within [Company]'s security operations, underscoring the need for ethical standards and robust oversight mechanisms in corporate settings.

This abbreviated summary chronologically outlines the events of the [Company] cyberstalking case, highlighting the severity of ethical misconduct and legal violations within the realm of corporate security.

Conclusion

Personal Sentences

- Sr. Director, age 47, sentenced to 57 months in prison, followed by two years of supervised release and a $40,000 fine.
- Director, age 50, sentenced to two years in prison, followed by two years of supervised release, and a $20,000 fine.
- Supervisor, age 56, sentenced to 18 months in prison, three years of probation, and a $15,000 fine.
- Sr. Manager, age 34, sentenced to one year and one day in prison and two years of probation.
- Analyst, age 28, sentenced to two years of probation, with one year to be served in home confinement.
- Analyst, age 28, sentenced to two years of probation, with one year to be served in home confinement, and a $5,000 fine.

Company Litigation

The victims of the cyberstalking are currently pursuing a civil lawsuit against the former CEO who is believed to be the beneficiary of the cyberstalking campaign because the victims had published content that was critical of him.

Discussion Questions

1. **Ethical Boundaries:** How do security practitioners define and maintain ethical boundaries in their work, especially when facing pressure from higher-ups or corporate interests?

2. **Responsibility of Leadership:** What responsibilities do security leaders have in preventing misconduct among their team members? How should they model ethical behavior?

3. **Corporate Culture and Ethics:** In what ways can the culture of a corporation influence the ethical decisions of individual security practitioners, and how can a toxic culture be identified and remedied?

4. **Legal Awareness and Compliance:** How should security leaders ensure that their teams are not just aware of legal boundaries but also committed to respecting them, particularly in high-stakes situations?

5. **Handling Whistleblowing:** If an employee in a security team witnesses unethical practices, what should be their course of action? How can organizations create a safe and effective process for whistleblowing?

6. **Conflict of Interest:** How can security practitioners navigate situations where their professional duties conflict with ethical considerations or personal morals?

7. **Training and Education in Ethics:** What role does ongoing training and education play in maintaining ethical standards within a security team?

8. **Crisis Management and Ethical Decision-Making:** In crisis situations, how can security practitioners balance the need for quick action with ethical decision-making processes?

9. **Long-Term Consequences of Unethical Actions:** What are the potential long-term consequences for a security team or organization that engages in unethical practices, and how can these be communicated to team members to deter such behavior?

10. **Public Perception and Trust:** How do high-profile cases of unethical behavior in the security industry, like this incident, impact public trust and perception of the industry, and what steps can security organizations take to rebuild and maintain this trust?

References

1. United States of America v. James Baugh and David Harville (2019)
2. https://www.justice.gov/usao-ma/pr/two-former-ebay-employees-sentenced-aggressive-cyberstalking-campaign
3. https://www.ncja.org/crimeandjusticenews/former-ebay-executive-gets-prison-term-for-cyberstalking-campaign
4. https://www.reuters.com/article/us-ebay-cyberstalking/former-california-police-captain-pleads-guilty-in-ebay-cyberstalking-case-idUSKBN27C23E/