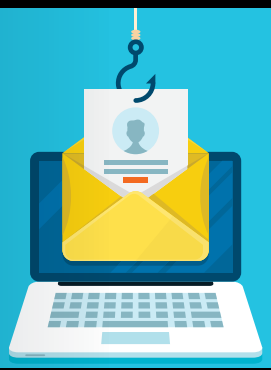
Redpoint
Cybersecurity LLC



BUSINESS EMAIL COMPROMISE (BEC)

THE CHALLENGE

Data breach incidents, including Business Email Compromise (BEC), are increasingly common today and affect businesses of virtually every size and in every industry. The motivations behind these attacks range from harvesting personal data (PII) to ransomware, wire transfer fraud, and general business disruption. Often these attacks begin with the compromise of a laptop or other mobile device, or on the endpoint (e.g. by means of phishing), so that the flow of malicious traffic is not "from the outside in" but rather "from the inside out." As more and more employees are working remotely the risk of compromise has exponentially increased.

TAB BRADSHAW
tab@redpointcyber.com
Chief Operating Officer
Redpoint Cybersecurity
www.redpointcyber.com

WHAT DOES A BEC ENGAGEMENT LOOK LIKE?

We bring the expertise to you. Redpoint's vast national security experience and technical acumen have been used to secure the world's most hardened operations. Redpoint can seamlessly transition any client's breach into the framework trusted and employed by the intelligence community. Our engineers use the NSA CIRA protocols in all of our breach response activities. Clients are afforded rapid on-site/remote investigative capabilities through the use of some of the most advanced technology platforms.

In reviewing Office 365 or email server configuration and audit logs, as well as email accounts, Redpoint engineers will:

- Look for **phishing attacks** and other suspicious activity;
- Attempt to **recover deleted messages** from the Outlook Data File of the impacted user;
- Analyze any **suspicious emails** sent or received from the victim inbox;
- Examine email provider logs and perform **header analysis**;
- Analyze **network traffic logs** for the customer's network;
- Examine **anti-virus logs** for unusual activity;
- Forensically collect all **suspect electronic storage devices**; and
- Conduct an analysis of the victim's computer system to determine if any **malicious software** was executed and installed.

Upon conclusion, the leadership across the organization will have a better understanding of cyber security and how to better secure their network from future attacks, and the client will move on to engage Redpoint's Threat Mitigation team, which will hunt for additional vulnerabilities and indicators of compromise and persistence.