

Blackbaud Cyber Security

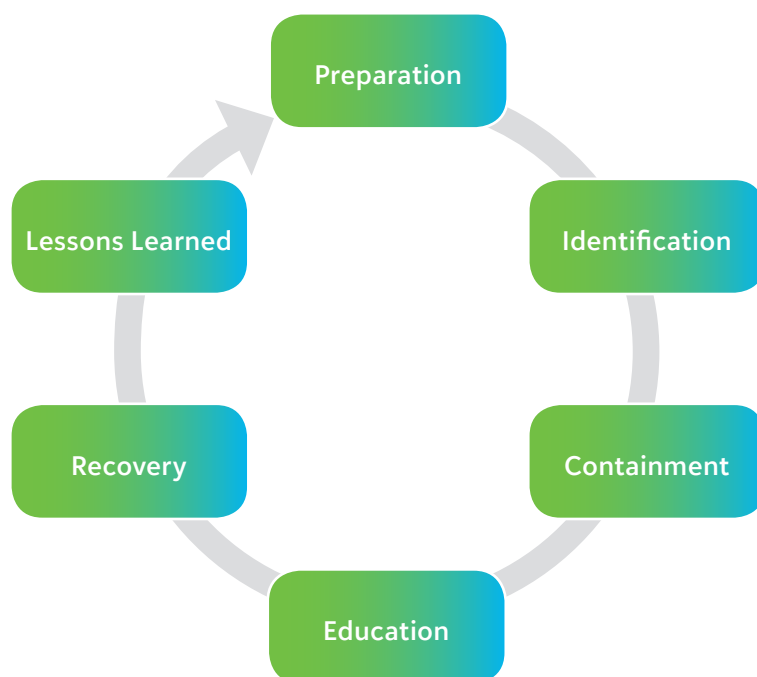
Incident Management and Response Overview



Operating in today's technology-enabled environment provides tremendous opportunity for Blackbaud and our customers to “do good” like never before. However, this opportunity comes with new and ever-changing risk. Cybercrime, fraud, data breaches, and Internet based adversaries can quickly disrupt a company's otherwise smooth operations. Attackers are constantly refining their tactics and developing new attack methods that place us all at risk. Blackbaud strives to implement and maintain a proactive and protective information security posture focused on avoiding or mitigating attack activity long before it presents a risk to our capabilities or customers.

Despite our continued focus and investment in cyber security, there may be occasions when an attacker is able to circumvent an existing security control or identify and exploit a new vulnerability. In order to ensure Blackbaud is well prepared in these situations, we maintain a dedicated incident response program aligned with industry standard practices to Identify, Contain / Eradicate, and Recover from inevitable security incidents. This document will provide a brief overview of this program and our approach to incident response.

The objective of Blackbaud's Cyber Security Incident Response program is to promptly and effectively mitigate the **impact** and **duration** of a security relevant incident. In order to accomplish this, we believe much of the hard work occurs long before an incident is ever identified – proper **preparation**. We regularly test the incident response plan via regular table-top exercises used to simulate potential attacks and response scenarios. This facilitates regular practice and continuously improves the incident response function. We also perform regular penetration testing to evaluate our preventative, detective, and responsive security capabilities.



** Cyber Security's incident response cycle*

This document outlines the Security related Incident response processes, but please note Blackbaud also maintains larger Incident Response & Crisis Management plans outside of the scope of Information Security.

© February 2020, Blackbaud, Inc.

This white paper is for informational purposes only. Blackbaud makes no warranties, expressed or implied, in this summary. The information contained in this document represents the current view of Blackbaud, Inc., on the items discussed as of the date of this publication.

All Blackbaud product names appearing herein are trademarks or registered trademarks of Blackbaud, Inc. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Identification

The identification of potential suspicious or malicious activity is accomplished by a dedicated team that collects, correlates, and analyzes diverse sources of security relevant data. This team performs comprehensive and continuous cyber security monitoring, and facilitates the identification of potential indicators associated with reconnaissance, attack, exploitation, system compromise, data exfiltration, etc. These indicators are evaluated for confidence, through the correlation of security relevant data sources. When a security incident is suspected, all relevant and ongoing support is provided to the Incident Response team. Emphasis during the identification phase is placed on the development of an attack hypothesis, unique and attributable information.

- Alert data provides key indicators of malicious activity through the use of threat signatures; behavior-based, and anomaly-based detection capabilities commonly provided by security platforms such as intrusion prevention systems, web application firewalls, security endpoint agents, and other tools.
- Event data is the vast dataset that includes observable and measurable activity that occurs on infrastructure, within applications, across the network, or at the endpoint. This data source is used to corroborate alert data or can be correlated to provide indicators of suspicious activity.
- Session data provides information about the nature of network traffic traversing Blackbaud's infrastructure. Awareness and analysis of this category of data can help the team identify anomalies or changes to a "normal" baseline of activity. Significant changes could indicate an incident and are investigated by the team.
- Packet data represents the actual content and "routing instructions" for data as it's passed from one point either across the Internet or within Blackbaud's network environment. This category

can be exceptionally helpful during an incident to determine the nature of an attack.

- Threat Intelligence provides Blackbaud's security analysts insight into the tactics, tools, techniques, and infrastructure used by attackers to initiate or support attack activity.

Through correlation and corroboration of these diverse sources of security relevant data, Blackbaud seeks to quickly identify a wide range of attack activity and initiate the incident response process.



** Cyber Security's relevant data sources*

Notification

In the event of a security incident, the response team will be notified through proper channels in a time frame that adheres to the latest compliance standards and Blackbaud contractual requirements.

Containment

When an incident occurs, the response team leverages security infrastructure to contain the spread and impact of an incident in order to minimize risk and maintain business operations.

Eradication

When an incident is successfully contained and can no longer impact other systems, the incident response team ensures affected systems are promptly returned to an original state and any attack vectors have been mitigated.

The incident response team focuses on eradicating any of the tools or application an attacker may have used. This includes malware, malicious scripts, unauthorized configuration changes, addition of accounts that may allow them to maintain “persistence”, etc. Any impacted systems still affected by the incident or response process are returned to a fully operational state and the incident response team convenes to perform an “after action” review.

After the incident response team conducts additional testing and monitoring, any containment measures that may have been put in place to constrain network traffic or system access are removed and systems are restored to their previous functional state. The threat vector, or path the attacker took, including vulnerabilities they may have discovered and exploited, accounts they may have accessed, etc. are remediated.

Recovery

Finally, after an incident is closed, the larger incident response team convenes to perform the “after-action” review. This exercise emphasizes continuous and iterative improvement through detailed scrutiny and analysis of incident response processes, preventative and detective controls, attacker tactics and tools, etc. The objective is for Blackbaud to continuously learn from all security incidents and integrate those lessons back into the program.

Conclusion

Blackbaud strives to maintain a cyber security posture focused on the proactive protection of products, infrastructure, and data.

We're committed to transparency and accountability around security incidents.

About Blackbaud

Leading uniquely at the intersection point of technology and social good, Blackbaud connects and empowers organizations to increase their impact through cloud software, services, expertise, and data intelligence. We serve the entire social good community, which includes nonprofits, foundations, companies, education institutions, healthcare organizations, and the individual change agents who support them.

