10-Point Agenda for a Post-Anthem Data Breach War Room

(by Secure Digital Solutions, LLC, © 2015 | trustsds.com)

What to Do	Who Should Do It
Define Scope and Team Identify systems that have access to sensitive data. E.g., databases, servers, devices. Identify any users (human or service credentials) that have access to these systems. Identify representatives of in-scope systems to support the exercise.	Operations management (e.g., CMDB owner), integration architects, IAM operations (IDP, entitlement management)
Review System Activity Include local logs, remote logs, current connections, current processes, etc. Look for failed and successful attempts to connect alike. Review firewall, gateway, proxy, and DNS logs. Review current activity both internally and outbound. Look for unusually large or lengthy sessions. Look for systems-to-system connections that no one can explain. Include batch and other non-web-based systems that handle large amounts of data. These systems tend to get less attention than web and mobile related environments even though the scope of data often dwarfs any other systems.	Administrators (sys admin, DBAs), SIEM team, anyone who can interpret the logs (e.g., integration architects), network operations team, network architects, network engineers, batch process owners
Perform Firewall Reality Check Review firewall rules. Test what host systems can actually reach. (Later, consider how to reduce network access to minimum necessary.)	Network operations team, network architects, network engineers, admins, integration architects
Check Behavioral Activity Review security monitoring tools (e.g., packet captures, behavioral logs, security gateways/proxies).	Security operations

1550 Utica Ave Suite 420 Minneapolis, MN 55416
main: 952-544-0234 www.securedigitalsolutions.com

Explain What's Found Review currently running and all installed applications on production systems. Can everyone explain what is running and why the application exists? (Later, consider how to reduce this to minimum necessary. E.g., do we really need a compiler on a production system?)	Operations, admins
Get Current Scans Scan the environment for vulnerabilities, perform baseline assessments (configuration, versions, etc.). Look for zero day vulnerabilities in particular. Patch or isolate systems that cannot be patched.	Security operations, IT operations, admins
Perform Attack Surface Reality Check Inventory admin consoles. Often these are not given a lot of attention, including during pen testing. Assume they are on every externally facing endpoint until it's proven they are not. Document how they are used and by whom. Consider closing off external access. Perform pen testing on those that are found. (Later, analyze all admin consoles, including internal and create policy and guidelines specifically focused on their design and deployment.)	Operations, application owners, application architects, application support, developers
Check Critical Credentials Review current service credential configurations. Review service credential process. Are they managed and rotated routinely? Consider rotating credentials for critical systems as part of the exercise.	Admins, IAM team, operations
Inventory Encryption Usage Review any clear-text transmissions (e.g., ftp, http, telnet, jdbc/odbc, etc.). Disable any externally facing cleartext protocols. Review encryption at-rest usage. (Later, enable encryption in-transit everywhere, internal and external.)	Network operations, admins, batch operations, application operations

1550 Utica Ave Suite 420 Minneapolis, MN 55416
main: 952-544-0234 www.securedigitalsolutions.com

Practice Breach Impact Analysis Identify attack patterns/scenarios similar to what is known about the breach in the spotlight. Generate system activity reports similar to what would be required when an attack has been uncovered. Can we show who accessed what data when and from where? If we had the IP of an attacker, could we show the scope of activity related to this IP? Can IP be traced all the way back to data access, or is the trail lost? (Later, get serious about log correlation, monitoring, and alerting. Don't just toss logs over the wall to the SIEM team.)	All from operations to IAM, from application admins to DBAs, from firewall to sys admin, from junior to senior leadership, SIEM team

Everyone:

- Keep an eye out for blind spots that might cause an attack to go unnoticed or make it impossible to determine the scope of a breach once an attack is uncovered.
- Conclude with a gap analysis with recommendations for improvement. Do we have glaring gaps, shelf-ware, or poorly utilized controls? What teams require more investment (staff and training)? What kinds of processes and tools should be explored to fill gaps?
- Make the case for highest priority investments with your executives, getting help from a third-party assessment for back-up evidence and arguments.

1550 Utica Ave Suite 420 Minneapolis, MN 55416
main: 952-544-0234 www.securedigitalsolutions.com