DELIVERING ON
DIGITAL

Confronting the Cybersecurity Challenge

Secure strategies

1. Identify the most attractive data targets for attackers. Gather your business leaders and threat intelligence experts and have them identify the top areas of cyber risk for your agency.

2. Use enterprise-level privacy officers to identify weak spots. Privacy officers can help determine which citizen data needs to be protected and why, by safeguarding citizen privacy and restoring trust when an incident occurs.

3. Monitor and audit third-party providers. Confirm vendors are complying with the data privacy and security stipulations in work agreements.

Vigilent strategies

4. Stay up to date on the full range of tactics attackers employ. Expect breaches to occur, and create multiple layers of protection to render some breaches harmless.

5. Identify potential external and internal threats and risk profiles. Step into the shoes of potential security threats to better grasp the precautions you need to thwart them.

6. Improve risk management through collective intelligence. Share information about vulnerabilities, threats and remedies to build a cyber-community of governments, enterprises and security vendors.

Resilient strategies

7. Create cyber-aware employee user experiences. Organizations that pay attention to user experience as they design their employee educational programs can quietly and unobtrusively guide users toward more vigilant and resilient behaviors.

8. Run simulations to glean insights on readiness. Conduct regular "fire drill" simulations on your system to understand its weaknesses and improve it continually.

9. Evolve defense mechanisms. Develop threat-monitoring plans for early detection of incidents and be prepared to respond when incidents do occur. Also have an effective recovery plan so that operations can be up and running quickly after a cyber incident.

10. Identify your cyberattack point person. Choose a crisis officer to run the response during an all-out cyberattack.

Stakeholder and talent strategies

11. Communicate the growing complexity of cyber threats. Clearly convey the nature and severity of cyber risks to agency and legislative leaders and other stakeholders.

12. Use private-sector partnerships to plug cyber skills gaps. Identify the skills and competencies you need to make your agency cyber-ready.

13. Make cybersecurity an attractive career option in government. Begin by mapping cybersecurity competencies and creating well-documented job descriptions.

Tools and techniques

14. Cyber wargaming. Create interactive cyber-attack scenarios and immerse potential responders in them to evaluate preparedness and identify deficiencies.

15. Attack graph. Understand vulnerabilities within the network by depicting the ways in which an adversary can break in.

16. Whitelisting. It allows only trusted content and software to run on your system.

17. Honey pots and honey nets. These are fake computer systems used to dupe attackers and collect information on intruders.

18. Penetration test. This is an intentional attack on a computer system to understand its weaknesses and find ways to gain access to its features and data.

www.deliveringondigital.com

Deloitte University Press

Deloitte. Digital

Delivering on Digital Deloitte 2016