TD Bank, U.S.

Survey Assessing Cybersecurity and Fraud Preparedness

Local governments are attractive targets for cybercriminals and particularly susceptible to cyberattacks because of the vast amounts of sensitive data they possess and maintain about infrastructure and the members of their community.

The goal of fraud controls and cyber security is to lessen the impact of a cyber incident on government entities of all sizes. Fraud and malicious cyber activity represent a serious and ever-increasing threat to financial resources, computer systems and critical infrastructure networks.

Questions for Government Leaders and Business Process Owners

1. Has your organization ever experienced a cybersecurity incident or breach?
   - ☐ Yes, we have experienced a direct incident.
   - ☐ Yes, a third party we contract with has exposed our organization.
   - ☐ We have had both direct and indirect incidents.
   - ☐ No
   - ☐ Unsure

2. Have you ever experienced a fraud incident?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

3. Which of the following types of financial fraud schemes are you familiar with? (check all that apply)
   - ☐ Account takeover fraud
   - ☐ Return Fraud
   - ☐ Chargeback Fraud
   - ☐ ACH Fraud
   - ☐ Wire Fraud
   - ☐ Checking fraud/ Fake checks/Whitewashing checks
   - ☐ Credit card fraud
   - ☐ Credit card skimming
   - ☐ Cloning a valid credit card
   - ☐ Identity theft

Katherine Heck | Vice President | Government Banking
143 North Main Street, Concord, NH
C:603-933-9997 |Katherine.heck@td.com

4. Which of the following types of payment fraud do you consider to be high-risk in terms of cybersecurity or fraud? (check all that apply)
   - ☐ Online Purchasing
   - ☐ Email scams
   - ☐ Texting scams
   - ☐ Telephone scams
   - ☐ Downloading files
   - ☐ ACH payments
   - ☐ ACH debits
   - ☐ Paper check cashing
   - ☐ Credit card -not -present fraud

5. Does your organization provide routine training around phishing, social engineering, online fraud, identity theft, malicious software, telephone/cell phone scams and more? (check all that apply)
   - ☐ Yes, regular training is provided on an ongoing basis for staff (Schools- for both staff *and* is part of the student curriculum).
   - ☐ Staff have access to self-guided training in protecting against email fraud and how to protect themselves online, if they choose to participate.
     - Schools- Students have access to self-guided training for defending against email fraud and how to protect themselves online, if they choose to participate.
   - ☐ There is a communication process for staff when suspicious activity or emails are identified.
     - Schools- There is a communication process for students when suspicious activity or emails are identified.
   - ☐ Some training is provided annually to both staff (and students, if applicable).
   - ☐ Unsure

6. Which of the following cybersecurity measures does your organization currently implement? (check all that apply)
   - ☐ Strong and unique passwords
   - ☐ Two-Factor Authentication
   - ☐ Regular software updates
   - ☐ Regular device updates
   - ☐ Using a firewall
   - ☐ Regularly Backing up important data

7. How often do you update passwords?
   - ☐ Monthly or Quarterly
   - ☐ Semi-Annually
   - ☐ Rarely
   - ☐ Never

Katherine Heck | Vice President | Government Banking
143 North Main Street, Concord, NH
C:603-933-9997 |Katherine.heck@td.com

8. How regularly are network security policies, password policies, secure wireless connections, encryption, remote access policies reviewed and updated?
   - ☐ More than once a year
   - ☐ Annually
   - ☐ As needed
   - ☐ Unsure

9. Does your organization have routinely updated network security measures in place to protect against unauthorized access?
   - ☐ Yes
   - ☐ No
   - ☐ Unsure

10. Does your organization have adequate controls around protecting sensitive data that includes personal information, data privacy, collecting data online and storage-both internally from unauthorized users and external threats?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

11. Does your organization have a incident response protocol in place in the event of lost or stolen data or a network breach?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

12. Does your organization have adequate controls around creating, making and approving payments and purchases?
    - ☐ We have written procedures including segregation of duties and dual controls in place to detect and/or prevent fraud.
    - ☐ We have an undocumented system, but adequate controls are in place to detect and/or prevent fraud.
    - ☐ We are too small to segregate duties or implement dual controls, but we have a system to monitor and prevent fraud.

13. What tool is your organization currently using to protect against check and ach fraud? (check all that apply)
    - ☐ Payee Positive Pay
    - ☐ Reverse Positive Pay
    - ☐ ACH Positive Pay
    - ☐ ACH Block/Filter
    - ☐ Check Block
    - ☐ Dual payment authorization

Katherine Heck | Vice President | Government Banking
143 North Main Street, Concord, NH
C:603-933-9997 |Katherine.heck@td.com

14. Does your organization regularly update procedures regarding electronic transactions, secure services, access to payment systems, protecting and storing credit card and customer data?
    - ☐ As needed when technology changes
    - ☐ Annually
    - ☐ Unsure

15. Have you identified your most critical government functions in your emergency management plans? (check all that apply)

    - ☐ stakeholders of critical operations and functions met to identify the processes and systems they oversee.
    - ☐ The processes and procedures have been documented.
    - ☐ Who is responsible for each of those processes, procedures and systems has been documented.
    - ☐ Critical government processes have been prioritized for the health and wellbeing of residents and staff (and students, if applicable) and for the protection of financial resources.

16. Do you have data backup processes (backups) in place for the most important systems to ensure the continuity of government operations? (check all that apply)

    - ☐ Yes, the backup strategy prioritizes critical government processes.
    - ☐ Yes, we have determined an acceptable level of data loss for critical business processes.
    - ☐ Yes, backups frequent enough to restore from data loss.
    - ☐ Yes, backups are tested regularly to ensure they work.
    - ☐ Yes, the backup process is documented.
    - ☐ Yes, the backup documentation accessible in the event of an emergency.
    - ☐ Unsure

17. Do you know who has access to the data and systems that support critical government functions? (check all that apply)

    - ☐ Yes, there is a list of internal users who have access to critical software and systems.
    - ☐ Yes, there is a list of numbers and contact information for vendors and service providers who have access to critical software and systems.
    - ☐ We do not have this information documented, but we know who has access.
    - ☐ Unsure

Katherine Heck | Vice President | Government Banking
143 North Main Street, Concord, NH
C:603-933-9997 |Katherine.heck@td.com