

Impact Self-Assessment

For each cell below, please indicate the *impact* to your organization if the party listed got access to that technology asset. **Leave blank** any rows that do not apply to you. Choose from the following:

- **Low:** Your organization would quickly recover with no long-term impact
- **Medium:** Your organization would be distracted for more than a week, face a limited reputational impact, or would incur significant costs in recovery
- **High:** Your organization would face serious regulatory, funding or constituent trust issues that would impact your organization for months or incur costs that could debilitate your finances

	<i>External Attacker</i>	<i>Internal Attacker</i>	<i>Concerned Citizen</i>
<i>Org financial account information</i>	<i>High</i>	<i>Low</i>	<i>Low</i>
<i>Staff HR data (salaries, SSN, etc.)</i>			
<i>Internal communications</i>			
<i>Internal intellectual property</i>			
<i>Constituent medical info</i>			
<i>Constituent financial info</i>			
<i>Donor or constituent contact info</i>			

There are also a few specific attacks that are looking less for your data and more to hijack your organizational resources for financial gain. Please indicate the impact on your organization of any of the following occurring. Again, **leave blank** any items that don't apply to you.

<i>Tricking staff into transferring money or sending sensitive HR information using misleading emails</i>	
<i>Ransoming servers through cryptoware</i>	
<i>Hijacking public website for disseminating malware or spam</i>	
<i>Stealing email account credentials for spam or fraud</i>	
<i>Repurposing servers, computers, or networking equipment for botnets or fraud</i>	

Prioritization Self-Assessment

The table below is color coded to reflect the *likelihood of a particular compromise* as **Common**, **Unusual**, or **Very Rare**.






Circling the boxes that you rated as **High Impact** on the previous page. Then number them in terms of priority to protect against starting at 1 (highest priority)






















	<i>External Attacker</i>	<i>Internal Attacker</i>	<i>Concerned Citizen</i>
<i>Org financial account information</i>	Common	Very Rare	Very Rare
<i>Staff HR data (salaries, SSN, etc.)</i>	Common	Very Rare	Very Rare
<i>Internal communications</i>	Very Rare	Common	Common
<i>Internal intellectual property</i>	Very Rare	Common	Unusual
<i>Constituent medical info</i>	Unusual	Unusual	Unusual
<i>Constituent financial info</i>	Unusual	Unusual	Unusual
<i>Donor or constituent contact info</i>	Very Rare	Common	Unusual






<i>Tricking staff into transferring money or sending sensitive HR information using misleading emails</i>	Common
<i>Ransoming servers through cryptoware</i>	Common
<i>Hijacking public website for disseminating malware or spam</i>	Common
<i>Stealing email account credentials for spam or fraud</i>	Common
<i>Repurposing servers, computers, or networking equipment for botnets or fraud</i>	Unusual

Vector Reference

The table below indicates the vectors that are **most likely** to result in compromise. The color coding continues to reflect the likelihood of such a compromise occurring.






-  **Identity Compromise:** Pretending to be someone else or stealing the credentials of a user with appropriate access
-  **Software Vulnerabilities:** Using compromised software to gain access to systems without credentials. Usually using known exploits that haven't been properly patched.
-  **Data Leakage:** Accidental exposure of data through storage in insecure locations or transmission via insecure means.
-  **Physical Access:** Gaining access to a physical device, usually to recover data stored on it
-  **Communication Interception:** Intercepting communications between parties or data in transit over the internet

	<i>External Attacker</i>	<i>Internal Attacker</i>	<i>Concerned Citizen</i>
<i>Org financial account information</i>			
<i>Staff HR data (salaries, SSN, etc.)</i>			
<i>Internal communications</i>			
<i>Internal intellectual property</i>			
<i>Constituent medical info</i>			
<i>Constituent financial info</i>			
<i>Donor or constituent contact info</i>			

<i>Tricking staff into transferring money or sending sensitive HR information using misleading emails</i>	
<i>Ransoming servers through cryptoware</i>	
<i>Hijacking public website for disseminating malware or spam</i>	
<i>Stealing email account credentials for spam or fraud</i>	
<i>Repurposing servers, computers, or networking equipment for botnets or fraud</i>	

Mitigation Reference

Below are the most effective techniques in addressing each kind of security. This is not intended to be a comprehensive list or include the options most suitable for all organizations.

	Mitigation	Effectiveness	User Impact	Difficulty or Expense	Value
Identity 					
	Multi Factor Authentication	Very Good	High	Low	High
	User Phishing Testing & Training	Good	Low	Low	High
	Advanced Logging & Monitoring	Good	Low	High	Moderate
	Policy, Training, and Culture	Good	Low	Low	High
Software 					
	Automatic Software updates	Very Good	Low	High	High
	Antivirus / Antimalware	Limited	Low	Moderate	Moderate
	DNS-Based Malware Filtering	Good	Low	Moderate	High
	Policy, Training, and Culture	Limited	Low	Low	Moderate
Data-leakage 					
	Remote Desktop or MDM	Very Good	High	Low	High
	Item Level Encryption	Good	Moderate	Moderate	Moderate
	Data Loss Prevention Monitoring	Good	Moderate	Moderate	High
	Policy, Training, and Culture	Good	Low	Low	High
Physical 					
	Building keycard systems	Very Good	High	High	Moderate
	Outsource to Cloud Provider	Very Good	Moderate	Moderate	High
	Computer Cable Locks	Limited	Low	Low	Low
	Device-level Encryption	Very Good	Low	Moderate	High
	Policy, Training, and Culture	Limited	Low	Low	Low
Communications 					
	Virtual Private Networks	Limited	Moderate	High	Low
	Firewalls & Intrusion Detection	Moderate	Low	High	Moderate
	Policy, Training, and Culture	Limited	Low	Low	Low

What's Next for Your Organization?

What questions do you still have?

What will you do to shift your organization's culture around security?

What technologies will you consider implementing?

What are you worried about now that you weren't worried about before? What is no longer such a concern?