If you're in government, then security is your business

Why cybersecurity is fundamental to your government operations

As the world becomes more interconnected, your government network and sensitive data become more vulnerable to unlawful access. Data breaches and ransomware attacks can cause devastating damage. Any successful attack brings with it the potential of financial loss, legal or regulatory infractions and brings harm to your organization's reputation.

Yet, despite the growing occurrence of cyberattacks, many organizations shield themselves behind a static and thin layer of protection. If your security culture is like many, you could be courting risky perceptions and improper security that open your operations to harm.

Find out what best practices are essential to securing your technology and maintaining optimal productivity.

Security Threats are Real and Constant

Protecting the cornerstone of government operations

From financial transactions to credentials, from documentation to records, countless daily business tasks rest on the confidentiality, integrity and availability of your technology and data. Whether you answer to tax-payers, patients, or the chain of command, you're expected—and often mandated—to safeguard that sensitive information and the solutions that house them.

The destructive impact of breaches

When your data and technology are threatened or compromised, productivity takes a nosedive, citizen trust suffers and expenses skyrocket. In 2018, the average global cost of a single data breach reached $3.86 million. In the face of such serious consequences, your organization may have implemented security protocols. But unless those initiatives are evolving and include multiple layers of defense, they may not be enough to mitigate attacks, especially as they're continuing to grow.

Cybercrime grows in size and force

To date, only five percent of hackers are being prosecuted.[3] A low rate of repercussions coupled with lucrative profits embolden bad actors to constantly search for weaknesses in your defense. As technology advances, their threats will only become more sophisticated and harder to detect. Take artificial intelligence. Tests from ZeroFOX have shown that artificial hackers are significantly better at composing and distributing phishing than their human counterparts. Add to that the boom of the Internet of Things (IoT), forecast to reach 50 billion devices by 2022.[4] To hackers, the proliferation of these smart, connected devices represent an expansive point of entry into your network and that of others.

Misconceptions lead to security mishaps

Although cyberattacks are front and center in the public eye, many government organizations operate under a false sense of security, lulled by misperceptions and inadequate measures. This paper aims to uncover those points of weakness and offer you strategies to fortify your security posture, without diminishing your productivity.

$3.86 million
average global cost of a data breach in 2018[1]

88% of hackers
can break through cyber security defenses within 12 hours[2]

41% of security firms'
network-based protections were circumvented[3]

54% of firms
responded to incidents involving consumer devices[3]

38% of firms
reported attacks involving enterprise devices[3]

Prevailing assumptions undermine protection

Are these viewpoints all too common in your workplace?

Attitudes influence the cybersecurity you implement and practice. Some employees feel their company's size is a sufficient barrier to hackers; others consider their network's firewall to be an acceptable shield. Then, there are those who cut corners because they see security as an annoyance that hinders productivity. Wherever you fall in the spectrum of viewpoints, know this: Cybercriminals are always searching for ways to bypass your security systems. If your security is not robust, deep and continually evolving, your technology and data are not well protected. It's wise to weigh the realities against the misperceptions, so you may bolster any frailties in your organization's security.

Myth: **We're protected by our network.**

Reality: **Traditional countermeasures such as firewalls and antivirus almost never slowed hackers down, but endpoint security technologies were more effective at stopping attacks.[2]**

How secure would your home be if you locked the front door, but not the windows or gate? A sound security plan is multi-layered and perennial.

Myth: **We haven't had a breach, so our security works.**

Reality: **A breach may have already occurred.**

Research shows that it can take a company as long as 197 days simply to detect a security breach.[1]

Myth: **We have a formal security program.**

Reality: **A one-and-done approach is too feeble to fend against expanding and emerging threats.**

Ask yourself if your program currently covers all of your technology connected to your network and data, including solutions, sensors, systems and enterprise devices.

Too often, those layers are overlooked. Then, assess how proactive your organization is in updating and evolving your security program. It needs to be as relentless as your foes.

Myth: **Security is too complicated.**

Reality: **Security that's well engineered is intuitive and easy to implement.**

Look for enterprise devices and solutions embedded with multiple layers of security, backed by proactive updates and supportive of rigorous security standards. They offer a metaphorical wall that protects your business. Their centralized, automated controls streamline IT tasks, while their intrinsic security works behind the scenes for end-users.

Myth: **Security hurts productivity.**

Reality: **A breach can bring work—and even worse, your business—to a grinding halt.**

One survey conducted by Ponemon Institute revealed just how much productivity can suffer at the hands of hackers:[7]

30% of surveyed enterprises lost IT and end-user productivity[7]

25% experienced system downtime[7]

23% experienced theft of information assets[7]

Fortify security with common sense best practices

What can you do to better protect your technology and data? Apply a battery of best practices to defend your enterprise devices and solutions. Mobile devices are inherently susceptible, when they are used outside of your firewalls, threat management, spam and content filters, and other tools intended to keep malice at bay. It's vital then that you minimize their exposure to risk via these effective methods.

Lastly, don't dismiss the importance of your staff. They can be your weakest or strongest link, depending on their willingness to comply. Raise awareness. Encourage participation by communicating the significance of security. Then, add teeth to your program by rewarding adopters and enforcing policies.

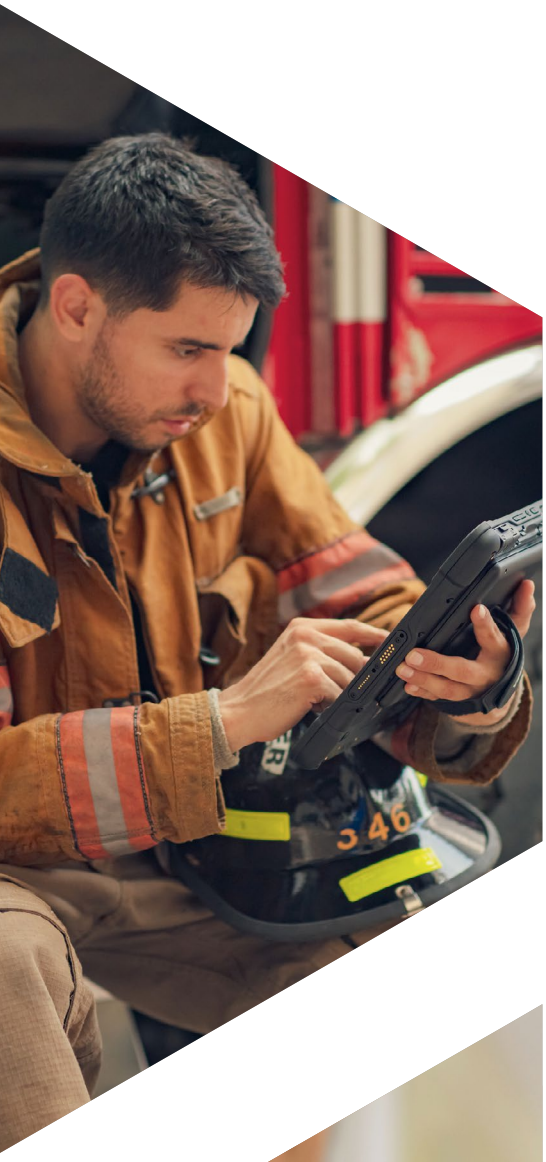
1. **Initiate a plan well in advance:**
   Modern technology offers exciting possibilities, as well as security risks. Take the time to define security protocols long before deploying your new solutions and devices.

2. **Protect Data:**
   Use encrypted and authenticated connections where possible, and encrypt data stored on your devices. While it's common to apply password and encryption to wirelessly connected devices, your wired/Ethernet-connected technology may need it too (dependent on the information it handles). Remember: If it's connected to your network, exercise caution.

3. **Control Services:**
   Many devices offer multiple communication methods. For example, network services can include FTP, SNMP and SMTP. While these services make accessing and managing the device easier, you may want to consider shutting them down if they're not in use.

4. **Change Passwords:**
   Defaults typically represent documented methods to access a device. Activate user-interface passwords. They should be strong and unique—in short easy for you to remember, but hard for others to guess. Forbid sharing credentials and require staff to change passwords after a set of time. It's important that you rotate your access passwords, access keys and authentication credentials.

5. **Use a Remote Management System:**
   This will allow you to quickly update settings. The longer devices, solutions and systems use outdated settings, the "easier target" they become. Remote management systems also considerably improve IT productivity, but their access and permissions should be carefully controlled.



6. Don't Advertise Updates:

Keep update schedules and plans only in the hands of those who need them. Knowing when updates are planned can inadvertently encourage inappropriate actions.

7. Monitor Out-of-Touch Technology:

Plan on having a method to continuously monitor your system for "out-of-touch" devices. When you suspect a device has been removed, withdraw its credentials until you can confirm its location.

8. Choose Devices That Can Be Updated, and Plan for Regular Updates:

Invest in devices that can be continually updated throughout their life cycle to ensure they remain current with new standards. It's also important that your update systems have the means to verify that update files have not been tampered.

9. Keep track of your technology:

Implement a retirement plan for your devices and solutions. This way you're sure to remove enterprise system settings, delete device user accounts and credentials and check that existing systems aren't hardcoded to search for retired units.

10. Consider the CIA Model:

During all stages of a device or solution's life cycle, it's wise to apply the confidentiality, integrity and availability model.

a. **Confidentiality:**
   Ensure only authorized personnel gain access to your technology and information.

b. **Integrity:**
   Maintain the consistency, accuracy and trustworthiness of data over its entire life cycle.

c. **Availability:**
   Finally, ensure that the device and data are available when the user needs them.

Introducing new technology should not introduce security risks

You invest in technology to enhance productivity and elevate efficiency. But assessing a technology's security should get equal footing, as it's critical to the well-being of your organization. Ask yourself if the solution and its maker invite or thwart security risks. Use these questions as a benchmark to gauge the strength of your enterprise technology.

1 Does the manufacturer adhere to globally recognized security best practices?

Not all do. Find out how stringent your technology provider's standards are. They should empower you to better monitor and respond to threats via tools, updates and support.

It's important you're able to act on each of these security steps, as laid out by a universally-accepted security organization's standards such as The National Institute of Standards and Technology Cybersecurity Framework:

- **Identify:** Evaluate and conduct a thorough risk analysis to uncover potential concerns
- **Protect:** Establish safeguards, policies and procedures; implement appropriate access and auditing controls
- **Detect:** Continuously monitor and audit your technology 24x7x365
- **Respond:** Establish a robust plan to analyze, triage and respond to detected events
- **Recover:** Organize a recovery plan-of-action; make improvements to course correct vulnerabilities and prevent future attacks

2 Is security embedded from inception to completion?

Built-in enterprise security mitigates risks. That's because it's engineered to give you complete centralized control over your devices and solutions. Enquire if you can lockdown the technology's home screen, features and peripheral interfaces, such as USB, Bluetooth®, GPS and near field communication (NFC). Look too for technology that offers government grade, granular data encryption.

3 Do they verify the security of their supply chain?

Without scrutiny over suppliers, how can you vet that the technology is designed as intended. In one case, a buyer found an unauthorized tiny microchip that could have created a stealth doorway to networks. Best to investigate the supply chain practices of your high-tech provider.

4 Is their security platform flexible enough to meet your operational needs?

Every organization is different. That goes for security tolerances. You'll want to set your own security levels and configurations depending on your company-wide and departmental needs. Keep that in mind when shopping for technology. Find out to what degree the solution offers you both flexibility and control.

5 Are continual updates and security support available throughout the solution's full life cycle?

Your security needs won't stop once you purchase your technology—and neither should your manufacturer's support. Threats are mercurial. They're constantly changing. How then can you stay ahead of the curve? Pick a provider that covers security updates for the entire life cycle of your technology.

6 Will they be proactive in evaluating potential security vulnerabilities?

Ideally, you're in the market for a security partner, not just a technology provider. A manufacturer worth their salt will inform you of emerging threats, offer advice on how to defend against them, assess your vulnerabilities and troubleshoot your business's specific areas of need.

7 Can they ensure rapid and effective response?

Should a vulnerability be identified, you need immediate and effective support. Look for a company that has a documented procedure for quickly reporting and responding to vulnerabilities. There should be proper resources available to rapidly investigate and remediate reported product vulnerabilities.

Zebra – Securing Your Performance Edge

Rely on Zebra products, services and solutions to be secure, without compromising performance. We take our role in securing your organization very seriously, because guarding against security vulnerabilities requires a proactive approach and multiple layers of protection. Zebra offers an entire portfolio of products that have undergone rigorous security reviews and validations such as the globally recognized Common Criteria Certification. Zebra also offers the broadest portfolio of rugged devices listed on the U.S. Federal Department of Defense Approved Products List.

Look around Zebra, and you can see our commitment to security in action. It's visible in our team of security, design and development professionals; our security framework; our secure supply chain practices and our assurance of ongoing preventative updates and customer alerts.

Easy to deploy and seamless to your frontline workers—our flexibility and features can be configured for your business to ensure both security and productivity. Our commitment is to engineer smart, configurable devices, solutions and services that allow you to balance operational and security objectives in real time, in the real world.

Count on Zebra to deliver secure solutions that won't hinder your performance, or the productivity of your frontline workers. It's peace of mind to help you implement your business and technology strategies at the edge.

Sources:
1. Ponemon 2018 Cost of Data Breach Study **2.** Black Report, Nuix 2017 **3.** Carbon Black Incident Response Threat Report, Nov. 2018 **4.** Juniper Research, 2018 **5.** Ponemon Institute, 2019 Cost of Data Breach **6.** Verizon 2018 Data Breach Investigations Report **7.** Ponemon 2018 State of Endpoint Security Risk

ZEBRA

Ask Us How You Can Feel and Be Safer

Visit www.zebra.com/product-security

COMMON CRITERIA