

CYBERSECURITY



Going Beyond The Mark!

# Is A Barcode Security Threat Looming In Your Company's Future?

- *Why Data Security is an Ever-Present Issue*
- *How Cybercriminals Access Your System and Data*
- *Results of an OS System Takedown & General IT Mayhem*
- *Methods for Preventing Barcode Cyber Attacks*



# IS A BARCODE SECURITY THREAT LOOMING IN YOUR COMPANY'S FUTURE?

By Shel Moore & Anne Roos

**A barcode scanner acts as a secondary keyboard to your computer. As it scans, data is quickly and accurately executed. Through a modern USB driver, barcode readers are as easy to install as a common PC keyboard.**

## The Security Threat Scenario

The simplicity of modern barcode reader operation opens the door to cyber threats. How easily can hackers gain access?

- Hyperchem Ma's demonstration at the PanSec Conference in Tokyo revealed that hackers can create automatic and advanced system-wide attacks, using ADF (Advanced Data Formatting), dialog attacks, and ASCII control characters through malicious barcode commands.

- Darren Kitchen and Shannon Morse's demonstration at the 2017 RSA Conference in San Francisco proved that the convenience and trust we have in barcode scanners is the cyberthief's trade. Hak5's "Rubber Ducky" USB device was distributed to attendees as a



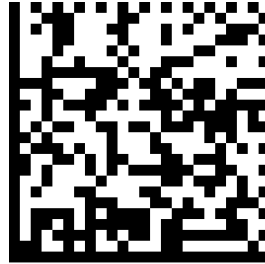
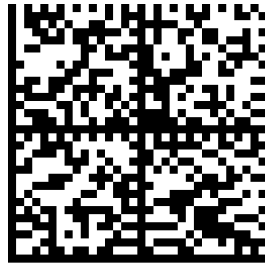
normal thumb-drive to display how it took over an operating system in just 15 seconds, looking like someone has plugged into a keyboard and was typing commands.

For the Rubber Ducky demonstration, participants were simply directed to a website containing useful advice on safe USB flash drive use. In reality, the repercussions to computer systems are very damaging,

# TRY OUR TEST.

## How safe are your readers?

Scan either of the two barcodes below. What happens next will depend on your scanner model. But for some common models, one of the codes below will auto direct your PC to open a website (in our example, it is NOT a malicious site). A similar normal-appearance bar code can be created for any company's scanner model.



Today's 2D barcodes are capable of storing upwards of 2000 keystroke characters. Examine the potential risk associated with each barcode symbology in our "How Secure Are Your Peripherals?" chart for the threat level associated with each barcode symbology.


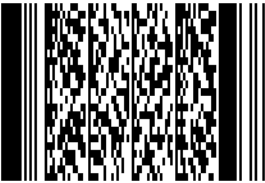


## TABLE OF CONTENTS:

*(Jump to the section you're most interested in.)*

- Consequences of A Security Breach
- Past Cyber Incidents Recorded
- Where Does the Sensitive Data Go
- Your Responsibility In the Event of a Breach
- Particular Laws That May Apply To Your Industry
- Preventing Cyber Attacks from Happening
- About ID Integration, Inc.
- Sources for More Information

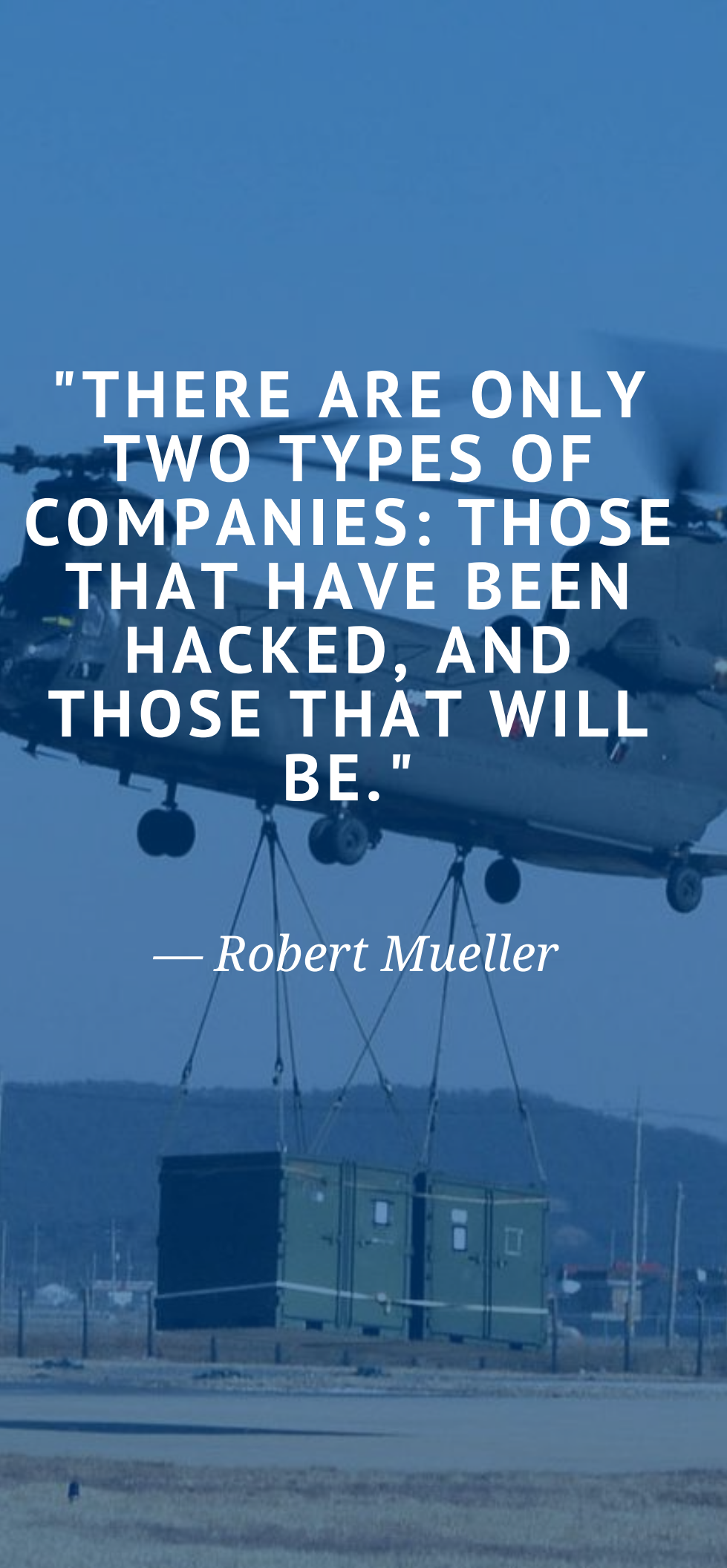


# How Secure Are Your Peripherals?

Barcode Symbology	# ASCII Characters Embedded	Popular Uses	Threat Level
 2D Data Matrix	1,556	Military IUID FDA UDI Military Shipping Label (MSL)	HIGH
 PDF417	1,108	Transportation Retail Document ID	HIGH
 QR Code	1,264	Marketing Information Events	HIGH
 Aztec	3,067	Asset Tracking Auto Tracking Registration	MEDIUM
 Maxi Code	93	Shipping Transportation	MEDIUM
 128 Linear	128	Medical FDA UDI Retail	LOW

From it, we can summarize that:

- 2D Matrix barcodes are at the peak of elevated risk. Increased data capacity heightens vulnerability.
- Basic linear barcodes, such as 128, have the lowest risk, due to limited data capacity, but can still generate an unwanted system-level command to your PC.

A large military helicopter is shown in flight, lifting a large, green, rectangular container or piece of equipment by a cable. The helicopter is positioned in the upper half of the frame, and the container is suspended below it. The background is a clear blue sky with some distant hills and a road visible at the bottom.

"THERE ARE ONLY  
TWO TYPES OF  
COMPANIES: THOSE  
THAT HAVE BEEN  
HACKED, AND  
THOSE THAT WILL  
BE."

—*Robert Mueller*

## **What are the consequences of a barcode security breach?**

At the outset, a malicious barcode could disable your system firewall, corrupt and/or delete files, and open port vulnerabilities, leading to future hacks. Recovery management by IT is an expensive undertaking—This entails patching holes in security, rebuilding operating systems, and updating and securing databases. The internal cost to recovering critical business function is immeasurable.

Malicious codes reap a host of consequences:

- **Botnets**—This collection of software robots creates an army of “zombie” infected computers that are remotely controlled by the cyber villain. Your computer may act as a zombie without your knowledge! Botnets spread malware, send spam emails containing virus attachments, and can take over your computer to attack other computers.
- **Distributed denial-of-service (DDoS)**—This attack occurs when a cybercriminal commands a network of zombie computers to sabotage a specific server or website. A DDoS attack can cause the complete shutdown of a website or server. By taking over your computer, a hacker could then instruct your computer to send massive amounts of spam to particular email addresses or send huge amounts of data to a particular website. A telltale sign that you may be a victim of a DDoS attack is when legitimate visitors to a website may be denied access.

- **Hacking**—This unauthorized access to your computer makes it easy for even non-technical people to take over your Win, Mac, and Linux keyboard through malicious barcode commands. Weaknesses, including pre-existing bugs and the lack of sufficient firewall protection, allow hackers to exploit your databases. Once they gain access to your operating system, hackers ensure a future of security breaches by installing a Trojan horse.

- **Malware**—This malicious software infects and damages your computer system. This general category of security threats includes computer viruses, spyware, adware, worms, and Trojan horses. It's primarily known for instructing your computer to display frightening pop-up windows that inform you that your computer has been taken over. In the meantime, malware reformats your hard drive, thus causing you to lose information, alter and delete files, and send emails that appear to be from you.

- **Ransomware**—This specific type of malware prevents you from accessing your computer and your computer files. The cybercriminal holds your system prisoner until you pay to have it released. Ransomware displays a notification on your computer screen that your data is locked and will demand payment to regain access. Sometimes the notification claims that you are in legal trouble and that you must pay a ransom to avoid prosecution.

- **Trojan Horses**—These malicious software programs install automatically once they are downloaded. They'll cause all manner of havoc, including deleting your files and then taking over your computer to hack other computers. They log your keystrokes, stealing sensitive data. They record names, usernames, passwords, and other sensitive information. Trojan horses allow cyber criminals to spy on you through your webcam.

- **Viruses**—Once downloaded, they infect your computer, and everyone's computer in your network and contact list. A virus can attack your hard drive and spread to USB keys and external hard drives. Any email attachment you create with your computer can infect computers that receive the attachment. Viruses provide cybercriminals with all-access to your computer, including contact lists, personal usernames and passwords, web browser, and security settings. They spew spam to your contact list and litter your screen with unwanted ads. The telltale signs of a virus take-over are many and various, depending upon which virus permeates your system. Assessing the type of infection and determining the cure involves a sizable time and money commitment from your IT team.

The profound consequences of a security attack cannot be understated. The extent of the ramifications may cost a company substantial expense and lost time.

## Cyber Incidents Recorded in 2016

82,000+ total cyber incidents in 2016 (Source: Online Trust Alliance)

90% of incidents could have been prevented (Source: Online Trust Alliance)

4,149 confirmed breaches worldwide (Source: Risk Based Security)

\$75 billion financial impact of ransomware (Source: The Atlantic)

35% rise in business-targeted ransomware (Source: Symantec)

1300% increase in business email compromise losses (Source: FBI)

58% increase in DDoS attacks (Source: Verisign)



**“EACH YEAR, COUNTLESS UNAUTHORIZED  
LEAKS CAUSE SEVERE DAMAGE TO OUR  
INTELLIGENCE ACTIVITIES AND EXPOSE OUR  
CAPABILITIES. THE FACT OF THE MATTER IS,  
SOME OF THE WORST DAMAGE DONE TO  
OUR INTELLIGENCE COMMUNITY HAS COME  
NOT FROM PENETRATION BY SPIES, BUT  
FROM UNAUTHORIZED LEAKS BY THOSE  
WITH ACCESS TO CLASSIFIED  
INFORMATION....THE INABILITY TO PROTECT  
OUR SOURCES AND METHODS FROM  
INTENTIONAL LEAKS CAUSES SUBSTANTIAL  
DAMAGE TO OUR INTELLIGENCE SERVICES  
AND NATIONAL SECURITY.”**

**— REP. PETER HOEKSTRA, FORMER  
MEMBER OF THE U.S. HOUSE OF  
REPRESENTATIVES**

## Where is all this sensitive data going?

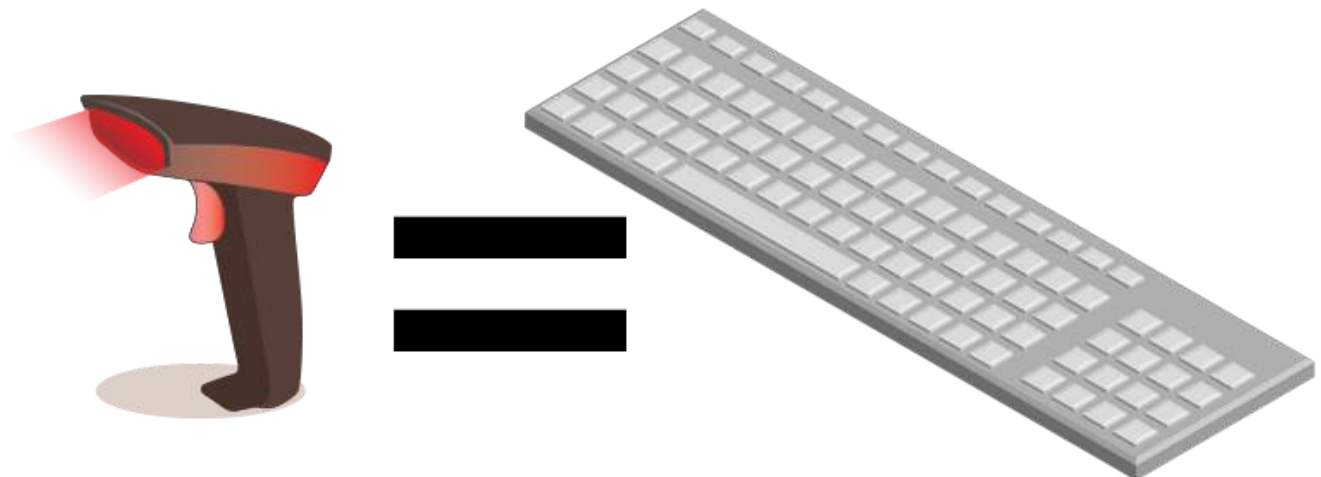
It's flooding the Deep Web marketplaces, otherwise known as the cybercriminal underground, with a great surplus of personally identifiable information: network administrator password credentials, hospital patient records, and military secrets.

"All organizations that 'process or store sensitive information are a potential target,' according to Numaan Huq, senior threat researcher at Trend Micro. 'By providing a better understanding of the nature of these attacks and how data is used throughout the process, organizations...can better protect themselves and be prepared to respond effectively if and when a breach occurs.'"

## Who does a barcode data breach impact?

Barcode scanners are pervasive in all industries. Here is just a sample of popular uses:

- FDA UDI label compliance for the tracking of recalls and the safety of devices
- DoD IUID marking and label compliance for military equipment and parts
- Medication tracking in hospitals to ensure correct dispensing and dosages
- Retail inventory and shipment analysis
- Barcode identity cards to monitor employee attendance and restrict access to facilities
- Barcode boarding passes



## Your Responsibility in the Event of a Security Breach

Regardless of your industry, your response to a cyber attack must be immediate to reduce the impact of financial, intellectual property, and credibility.

Create a written Cyber Incident Response Plan to identify specific attack scenarios paired with appropriate responses to each type of attack. When a potential breach is reported, your response team goes to work to halt the cyber intrusions from spreading while documenting the investigation.

After this initial assessment, follow up with a detailed internal investigation to gain a better understanding of the type of computer breach, to identify the attacker, to detect and resolve any security vulnerabilities, and to identify improvements to prevent future breaches.

After a breach, notice must be given to the following entities, depending upon the State and Federal laws that apply:

- State and Federal agencies and regulators of cyber breaches
- Clients, contractors, customers, and consumers whose information was breached
- Your insurers
- Law enforcement



## Particular laws may also apply to your industry:

- The Health Insurance Portability and Accountability Act (HIPAA)—When you belong to the “covered entities” or “business associates” categories that handle “protected health information” (PHI), you and your company are required to be compliant. Violations take many forms.

According to Jason Karn, Chief Compliance Officer for Total HIPAA Compliance, “Ransomware costs organizations \$209 billion in the first quarter of 2016 alone...It costs \$380.00 per record to try to mitigate a breach.”

HIPAA states: “The penalties for noncompliance are based on the level of negligence and can range from \$100 to \$50,000 per violation (or per record), with a maximum penalty of \$1.5 million per year for violations of identical provision. Violations can also carry criminal charges that can result in jail time.”

These repercussions can also extend to civil liability suits, on top of levied financial and criminal punishments.

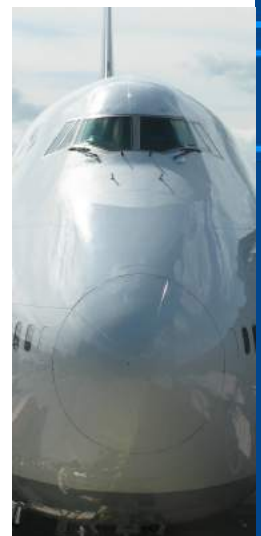
- The Department of Defense Final Rule on Defense Industrial Base (DIB) Cybersecurity (CS) Activities—As of October 4, 2016, this rule “implements mandatory cyber incident reporting requirement for DoD contractors and subcontractors who have agreements with DoD. The mandatory reporting applies to all forms of agreements between DoD and DIB companies (contracts, grants, cooperative agreements, other transaction agreements, technology investment agreements, and any other type of legal instrument or agreement).”

This rule was developed as a part of a large effort to secure government contractors in the DOD’s DIB information-sharing network. DIB members can exchange both classified and unclassified data on hacking threats.

The Final Rule followed the August, 2015 White House release of a set of guidelines that require contractors that handle sensitive data to achieve baseline security requirements and report digital breaches to authorities.

- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations—On December 20, 2016, The National Institute of Standards and Technology (NIST) published this Revision to Special Publication (SP) 800-171: A System Security Plan (SSP) must “describe the boundary of [a contractor’s] information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems.”

With the staggering costs involved over work stoppage, investigation of the extent of the breach, repairing systems and data, and reporting to legal entities, an ounce of prevention equals a pound of cure.



# CONCLUSION

## PREVENTING CYBER ATTACKS FROM HAPPENING IN THE FIRST PLACE

How can you guarantee that your barcodes safely pass compliance with good data? Without security filter protection, your data runs the risk of corruption by barcodes embedded with malicious codes.

The team at ID Integration, Inc. realizes that there are many ways to protect network systems through restricted access, limited workstation functions, etc. These experienced systems integration professionals also recognize the hazards and surprising nature of security risks throughout the warehouse and shop floor. Especially those risks, which may not be assessed as a standard IT function due to the reliance of manufacturing equipment provider assurance.

As an independent integrator, ID Integration is poised in a unique position to develop hands-on, real world experience with a comprehensive range of automation and data tracking hardware and software solutions – that are not tied to specific manufacturers or products. These custom-tailored analyses and recommendations are made with each clients' best interests at heart. The hidden and critical nature of today's barcode security threat impacted the team at ID Integration to the point they felt an urgency to develop an effective and easy to use means of protection. As an alternative to the inconveniences associated with mitigating protection: removing ASCII character recognition from barcode scanners, limiting workstation functions, restricting internet browsing access, among other methods, ID Integration has created their patent-pending BarCode<sup>OS</sup>® security filter – the first and only of its kind.

It is not a realistic solution to restrict the ability of barcode scanners from reading ASCII codes. This ultimately renders the hardware useless in contributing to modern-day asset tracking and automation applications. BarCode<sup>OS</sup>® enabled scanners present a solution that is simple, smart, and secure for all industries. They also deliver enhanced modules tailored specifically for unique and challenging applications within the DOD military IUID, FDA UDI, and other market spaces.

**BarCode<sup>OS</sup>® enabled scanners put a stop to security threats using the FIREWALL technology advantage:**

- BarCode<sup>OS</sup>® enabled scanners are equipped with the World's only data security filter to halt malicious operating commands. Malicious 2D Data Matrix, free-form QR, and PDF417 barcodes are stopped in their tracks. (The BarCode<sup>OS</sup>® Data Security Filter is Patent Pending.) This firewall protection is not limited to just Windows operating systems.
- BarCode<sup>OS</sup>® enabled scanners use a simple audible alert to sound the alarm when scanning invalid syntax codes: Just one beep tells you the barcode is good, while four beeps signal an invalid data syntax has been used in the code (DOD, Healthcare, ID card standards are supported).

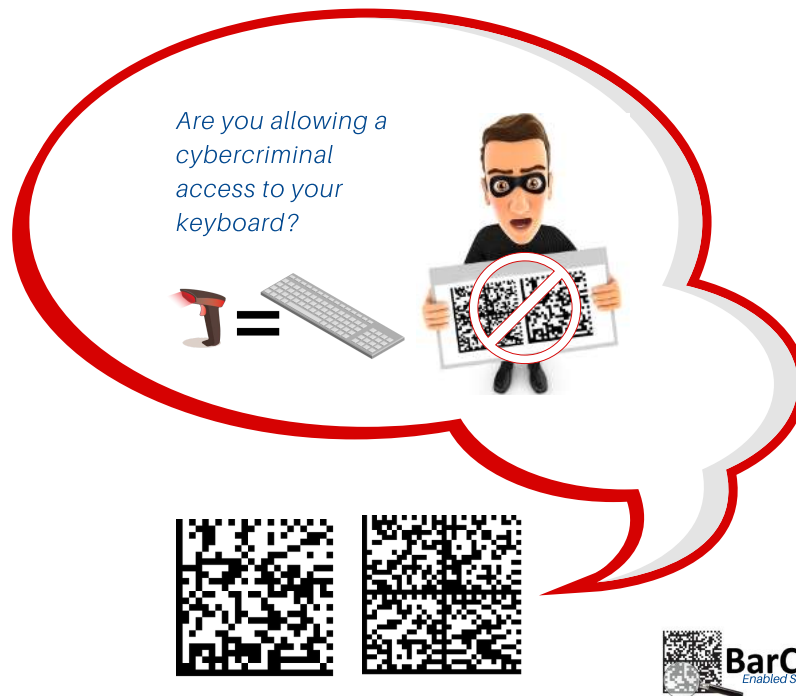


Five beeps indicate that a malicious barcode has been identified and blocked.

- BarCode<sup>OS</sup>® enabled scanners read any supported barcode, even malicious codes, without the danger of infecting your computer and network. You'll get a "rogue barcode disabled" message in the reader's display to assure you that dangerous run commands are completely stifled. For non-display reader models, five rapid beeps are used to notify that a malicious barcode has been identified and blocked.
- BarCode<sup>OS</sup>® enabled scanners employ file encryption to block tampering or disabling of this security filter – positioning BarCode<sup>OS</sup>® scanners as the world's most secure hardware platform available today.

Get started with BarCode<sup>OS</sup>® enabled scanners, customized to fit your industry application. Protect your computer, operating system, network, and data with the only Firewall protection that blocks threats hiding within malicious barcodes.

## How Many *Keystrokes* Would It Take?!



### ABOUT ID INTEGRATION, INC.

ID Integration is a seasoned systems integrator with over two decades of experience in complex U.S. Department of Defense IUID, FDA UDI, ATA SPEC2000, and a wide range of asset tracking and automation applications for the aerospace, military, government, and medical industries. Past and current clients include industry leaders like the U.S. armed forces, Boeing, Lockheed Martin, Honeywell Aerospace, Northrup Grumman, Raytheon, United Airlines, and others.

Recently, ID Integration has expanded their service offering to provide enhanced consulting for cybersecurity that partners with IT departments within the manufacturing, logistics, and industrial market space. Their experts provide full-service systems integration that's mindful of automation, tracking, and compliance needs while also managing existing and emerging cybersecurity threats.



Request a cybersecurity needs survey for a thorough analysis of current systems – from the office to the shop floor – and everything in between. The team at ID Integration, will review your asset tracking, automation, and compliance processes by examining your software, hardware, and network connections to identify potential threats. You'll receive a detailed analysis report that highlights existing risks, provides recommendations for resolution, and all with expertise from a team with the experience and know-how to implement the prescribed protective solutions.

### Sources:

"Cybercriminals Now Using Barcode Security Threat": <https://id-integration.com/barcode-security-threat/>

"Intelligent Scanners": <https://id-integration.com/intelligent-scanners/>

"2017 Cyber Incident & Breach Response Guide" published by the Online Trust Alliance: [https://otalliance.org/system/files/files/initiative/documents/2017\\_cyber\\_incident\\_breach\\_response\\_guide.pdf](https://otalliance.org/system/files/files/initiative/documents/2017_cyber_incident_breach_response_guide.pdf)

"5 Consequences of an Information Security Breach": <https://www.besttechie.com/5-consequences-information-security-breach/>

"AusCERT 2017 – You Are the Universal Attack Vector" keynote presentation by Darren Kitchen and Shannon Morse: <https://www.cso.com.au/article/619967/auscert-2017-universal-attack-vector/>

"BadBarcode: How to Hack a Starship with a Piece of Paper" presentation by Hyperchem Ma: <https://www.slideshare.net/PacSecJP/hyperchem-ma-badbarcode-en1109nocommentfinal>

"Common Threats To Be Aware Of": <https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx>

"Cyber Attacks: Prevention and Proactive Responses", by Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP: <https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf>

"Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim" by Wayne M. Alder: [http://www.becker-oliakoff.com/webfiles/pdf/alder/20151001\\_alder\\_data\\_breaches.pdf](http://www.becker-oliakoff.com/webfiles/pdf/alder/20151001_alder_data_breaches.pdf)

"Data Security Breach Notification Laws", by Gina Stevens, Legislative Attorney: <https://fas.org/sgp/crs/misc/R42475.pdf>

"Dispelling Data Breach Myths", by Sally Cole: <http://mil-embedded.com/articles/dispelling-data-breach-myths/>

"HIPAA and the Risks of a Data Breach": <https://book4time.com/hipaa-risks-data-breach/>

"The DOD Now Requires Contractors to Report Hacks" by Cory Bennett: <http://thehill.com/policy/cybersecurity/255757-dod-now-requires-contractors-to-report-cyber-breaches>