



DittoCast
Data Breach Prevention

7 Critical IT Security Protections EVERY Business Must Have In Place NOW

To Avoid Cyber Attacks, Data Breach
Lawsuits, Bank Fraud and Compliance
Penalties

Provided by
Global Access Incorporated
(866) 809-0399
<https://DittoCast.com>

Global Access Incorporated
660 Fitzhugh Blvd, Smyrna, Tennessee 37167
(866) 809-0399

(DittoCast® is a registered trademark of Global Access Incorporated, Copyrights 2018)



DittoCast
Data Breach Prevention

We're Going To Cover

The #1 Security threat to your business that antivirus, firewalls, behavior monitoring, and other security protocols can't protect against.

A shocking truth about bank fraud that most businesses don't know about that could literally wipe out your bank account.

Why firewalls and antivirus software aren't enough anymore.

How mobile phones and cloud applications are seriously jeopardizing your organization's security and data protection and what you need to do to protect yourself.

Plus, to help protect your business against today's cyber threats we have a special, Free offer.

Ultimately, we're going to cover...

How to avoid being Sitting Duck to cyber criminals and protect everything you've worked so hard to achieve.



Global Access Incorporated

660 Fitzhugh Blvd, Smyrna, Tennessee 37167

(866) 809-0399

(DittoCast® is a registered trademark of Global Access Incorporated, Copyrights 2018)



DittoCast

Data Breach Prevention

This is a new world of technology we live in and 'only the paranoid survive', according to Andrew Grove, previous CEO of Intel.



There is a Digital Underground **Black Market**

Also known as the **Dark Web**. Where ...

- Credit card details sell for \$2-\$90
- iTunes accounts sell for \$8
- Physical credit cards for \$190
- Card cloners for \$200-\$300
- Fake ATM machines for \$35,000
- Entire personal online identity \$1,200
- Online shopping accounts, Amazon, Ebay, Walmart for \$165
- Online travel accounts, Expedia, Uber, Airbnb for \$45
- Netflix, Spotify, etc for \$29
- Social media accounts sell for \$10

Ok, so you may be thinking right now this would never happen to us, we're too small or we're too big or our IT guys have it handled!

WRONG!

One in five small businesses fall prey to cyber crime and it's growing. Small businesses are easy 'low-hanging fruit' because of their complacency, over confidence and inconsistent security practices. Just because you're small doesn't mean your customer's data is any less valuable. What are you doing to protect your customers?

Five out of six large companies, with over 2,500 employees, are targeted by cyber criminals, which has recently increased by 40% in one year. Most attacks are finely tuned phishing and fraudulent email campaigns plus over 1 million malware threats each DAY!

Here's what your life would be like **after a Data Breach...**

- Reputation damage
- Loss of clients

Global Access Incorporated

660 Fitzhugh Blvd, Smyrna, Tennessee 37167

(866) 809-0399

(DittoCast® is a registered trademark of Global Access Incorporated, Copyrights 2018)



- Class action lawsuits
- Individual lawsuits
- Legal fees
- Government and State compliance penalties
- Replacement of data
- Major systems downtime, loss of productivity

Furthermore, the FDIC (Federal Deposit Insurance Corp) **does not** protect you from Bank Fraud and the **Bank is NOT responsible** for getting your money back if taken by fraud or identity theft.



Tips for Protecting Your Business Bank Accounts:

- Cancel debit cards; they are the #1 way bank accounts get compromised. Instead use true credit cards such as American Express, etc.
- Have a dedicated PC for online banking and DON'T use that PC for accessing any other web sites, email, social media sites or for downloading files or applications.
- Sign up for e-mail or text alerts from your bank whenever a withdrawal over \$100

happens.

- Require YOUR signature for any wire transfers.
- Spread your money out in multiple accounts so the risk of having one large money account wiped out is minimized.

Over 600,000 Facebook accounts are hacked every single day making Social Media the #1 Threat today.



Consider blocking access to social media sites for users at work to reduce that threat and to resolve the #2 business Threat, **Significant Loss of Productivity.**

Percent of Employees (weekly)	Hours (weekly)
39%	<1 hour
29%	1-2 hours
21%	2-5 hours
8%	6-10 hours
3%	10+ hours

Contributing to this loss of productivity are social media, Tumblr (57%), Facebook (52%), Twitter (17%), Instagram (11%) and SnapChat (4%).

In addition, Threat #3, **antiquated business systems, processes and software** contributes huge losses in productivity and exposure to attack. Most all businesses have built critical operating processes around older technologies such as, email. Offered to the public in the early 1970's, email was designed to drop a message from one computer to another across an external network. The creators never thought about hacking, malware and viruses, therefore **email was never designed to be secure.** In fact, computer viruses didn't show up until 10-15 years after email began. Email has been critical to business communication for 30+ years, however the risk and productivity loss from email threats has greatly diminished its' value. We are now at a risk versus cost tipping point which is motivating businesses to look for other solutions. These solutions are paving the way for relief from risk, more productive operations and higher profitability, from cloud based secure messaging and hybrid email processing systems with integrated secure file sharing. These allow communication by traditional methods while your business transitions to safe and highly productive messaging solutions giving executives more control and a much-needed peace of mind.

It's **time to re-evaluate your IT solutions** whether it's antiquated antivirus filters, email or customer accounting.

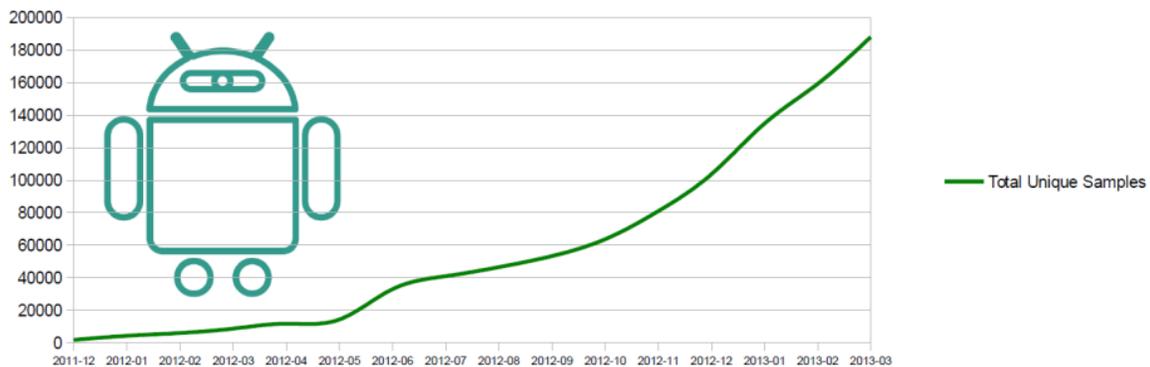


Social Media – Public Relations Threat

Any publicized cyber-attack, social media post, or stupid employee stunt like the Burger King kid taking pictures of himself standing in the lettuce bins then posting to social media can greatly damage a business. Given the rampant use of social media, Public Relations departments must keep an eye out for such devastating posts, thus making Bad PR a serious threat #4.

The Next Frontier: Mobile

Mobile malware growth is accelerating, the mobile computing dangers are on the rise...



If a device is lost or stolen and the data was NOT encrypted you may have violated a Data Breach Law. In many states, personal information, that must be protected is as basic as first and last name, a combination of last name and driver license number, social security number, log on or passwords.



For the first time, a small data breach draws a big fine (\$50K)

Idaho hospice to pay \$50,000 for HIPAA violation

By [Paul McNamara](#) on Mon, 01/07/13 - 10:22am.

17 Comments Print Share 75 +1 Like 95 More

Losing a single laptop containing sensitive personal information about 441 patients will cost a non-profit Idaho hospice center \$50,000, marking the first such penalty involving fewer than 500 data-breach victims.

The data was unencrypted.

The Department of Health and Human Services (HHS) announced last week that it has reached an agreement with the [Hospice of North Idaho](#) that will see the hospice pay \$50,000 for violating the Health Insurance Portability and Accountability Act (HIPAA).



Global Access Incorporated

660 Fitzhugh Blvd, Smyrna, Tennessee 37167

(866) 809-0399

(DittoCast® is a registered trademark of Global Access Incorporated, Copyrights 2018)



DittoCast
Data Breach Prevention

How to Protect Your Business

7 Critical IT Security Protections

- 1) Create a solid UTM (unified Threat Management) plan incorporating multiple layers of protection.
- 2) Update business software, not only operating systems, but email, accounting, CRM, point of sale terminals, firewalls, wifi systems and routers.
- 3) Evaluate and lock down use of risk laden applications such as email, drop box file sharing, instant messaging, texting, social media, etc. Look for 'real' security not just going by the marketing materials for a product, ask the hard questions. 'How does it work?' 'Where are the private keys stored?' 'How are private keys protected?' 'What are the security features of your servers or data center?'
- 4) Control what web sites employees can access.
- 5) Force a strong password policy for all devices with difficult to hack format.
- 6) Eliminate employee remote access unless thru a tightly controlled VPN (Virtual Private Network) device. Don't allow 'coffee shop' access from public wifi.
- 7) It seems logical however many businesses do not have adequate backups of data and applications that can be used recovering from malware and ransomware attacks.

Global Access Incorporated

660 Fitzhugh Blvd, Smyrna, Tennessee 37167

(866) 809-0399

(DittoCast® is a registered trademark of Global Access Incorporated, Copyrights 2018)



DittoCast
Data Breach Prevention

It's Time to Get Serious About Protecting Your Business and Customers

➤ **Threat assessment**

What is lacking in your security plan now?

How are employees using company-owned or personal devices?

Identify what 3rd party services or applications you are using?

Test your backups?

Where is your greatest exposure to risk?

Who's responsible for your network security and are they doing it?

➤ **Action Plan**

Based on the assessment discovery what's the plan to ensure your systems, data, customers, operations, software and facility is safe from any type of risk?

➤ **Maintenance Plan**

'Set it and forget it' is not a plan. Develop a relationship with a solid IT company for accountability whether you have an inhouse IT department or not. Make sure someone is responsible and reports on his/her activity to ensure it's done and done well.

THE FIRST ASSESSMENT STEP IS FREE

At no cost or obligation, we will provide you a search of the Dark Web for all employee's company credentials.

This will assist in identifying the current risk level and effectiveness of your current security. Every plan needs a goal or target to shoot for, the Dark Web scan will provide needed information for establishing that goal.

Global Access Incorporated

660 Fitzhugh Blvd, Smyrna, Tennessee 37167

(866) 809-0399

(DittoCast® is a registered trademark of Global Access Incorporated, Copyrights 2018)



DittoCast
Data Breach Prevention

THINGS YOU NEED TO KNOW

- 1) We can only offer the FREE Dark Web search to businesses with 50 or more employees.
- 2) We never want to leave you out, so if you have fewer than 50 employees, we have a one-time search cost reduced to \$89 plus have waived the \$300 setup cost!
- 3) There is NO Obligation to buy anything or further costs.
- 4) We do offer additional services to assist in securing your business and will gladly provide you with more details.

To Get your scan of the Dark Web offer, click the link below, complete the sign-up form so we can contact you with the full report.

[Https://Dittocast.com/DarkWebScan](https://Dittocast.com/DarkWebScan)

Global Access Incorporated

660 Fitzhugh Blvd, Smyrna, Tennessee 37167

(866) 809-0399

(DittoCast® is a registered trademark of Global Access Incorporated, Copyrights 2018)