
WHAT'S YOUR FIRMS **SECURITY** STRATEGY?

MODERN LAW OFFICE

**THE I-WORX
TRUSTED
CLOUD**



Security Is Top of Mind

AS FOR THE PRIVATE SECTOR:

90%

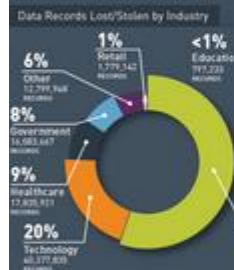
of businesses have been hit by a cyber security breach in the past year.

41%

Breaches cost 41 percent of businesses at least \$500,000.



THE TOP TWO DEVICES UNDER ATTACK ARE LAPTOPS AND MOBILE DEVICES.



Today's attackers act quickly



2015 SECURITY PREDICTIONS

This year's headlines made it clear: the number of devastating cyber-attacks is increasing and the costs aren't just financial. Every data breach can irreversibly damage an organization's reputation, a priceless commodity. In this high risk threat landscape, protecting your data from malicious attacks requires not only the right tools, but a pre-emptive awareness of the latest threats and tactics. Below are WebSense's 2015 Security Predictions - eight critical cybercrime trends that will challenge IT security professionals everywhere.



HEALTHCARE HACKS WILL ESCALATE.

Highly valuable Personal Identifiable Information (PII) in healthcare databases will make the industry a prime data theft target. Insurance company, pharmaceutical, hospital and doctor office networks will provide multiple potential entry points for hackers.



INTERNET OF THINGS (IOT) ATTACKS WILL FOCUS ON BUSINESSES, NOT CONSUMERS.

More than sixteen billion devices will be connected to the Internet by 2015 and will double to more than forty billion devices by 2020. As the attack surface increases, so does the "noise" that must be accurately filtered to identify true threats.



CREDIT CARD THIEVES WILL EVOLVE INTO "INFORMATION DEALERS" FOR THE BLACK MARKET.

Cybercriminals will serve as "one-stop shops" for identity theft and financial fraud, with operations harvesting information from a variety of sources. As a result, two-factor authentication will become more commonly required to prevent unauthorised access to data.



MOBILE THREATS WILL TARGET CREDENTIALS.

be targeted loud-based ions and data l by mobile igh auto-login site apps.



UPGRADING SECURITY IS AMONG THE TOP FOUR PRIORITIES THAT CEOs HAVE FOR THEIR CIOs IN THE COMING YEAR (UP FROM #8 LAST YEAR).

85%

of U.S. tech executives are taking steps to increase IT security in 2015

66%

of Security Professionals Believe They Will Suffer a Data Breach within the Next Three Years

[1 IN 5]

ENTERPRISE SECURITY PROFESSION Would Not Entrust Their Personal Data their Own Networks

Cost of Security

Financial consequences of a security breach may range from fines levied by regulatory authorities to brand erosion.

\$90 - \$305

The average security breach can cost a company between \$90 and \$305 per lost record, according to a new study from Forrester Research.

FORRESTER

\$416,000

The average average cost

Rebuilding a brand can cost millions in

- 1 public relations consulting fees
- 2 customer outreach efforts
- 3 advertising campaigns
- 4 defending a company in the face of liability suits

SECURITY INCIDENTS INCREASED 33% LAST YEAR

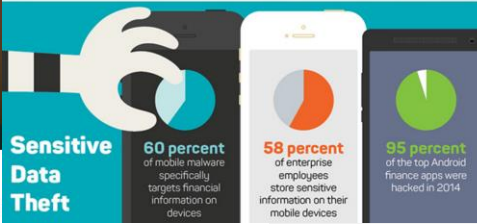
FEATURE iOS vs. Android: Which is more secure?



When it comes down to actually protecting enterprise users, is one mobile operating system - Android or iOS more secure than another?

MEET THE MOBILE MENACE

TOP THREATS TO MOBILE SECURITY AND WHAT YOU CAN DO TO PREVENT THEM

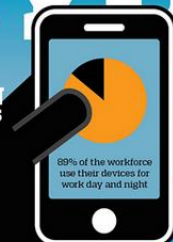


THE HIGH COST OF BYOD

1.2 BILLION SMARTPHONES will enter the market over the next 5 years



That's 40% of all handset shipments



80% of the workforce use their devices for work day and night

75% OF COMPANIES allow employees to use personal devices at work



That'll rise to 90% by 2014

Mobile Security: Low

MALWARE EVERYWHERE
SURVEYING SECURITY PROFESSIONALS ON WEB, EMAIL AND SOCIAL THREATS

What's Driving Security Challenges Today?

Reputation



Regulatory Compliance



Breach Response



Special Cases



Nation-state



Industrial Espionage

Everyday



Insiders



Disruptive Technologies

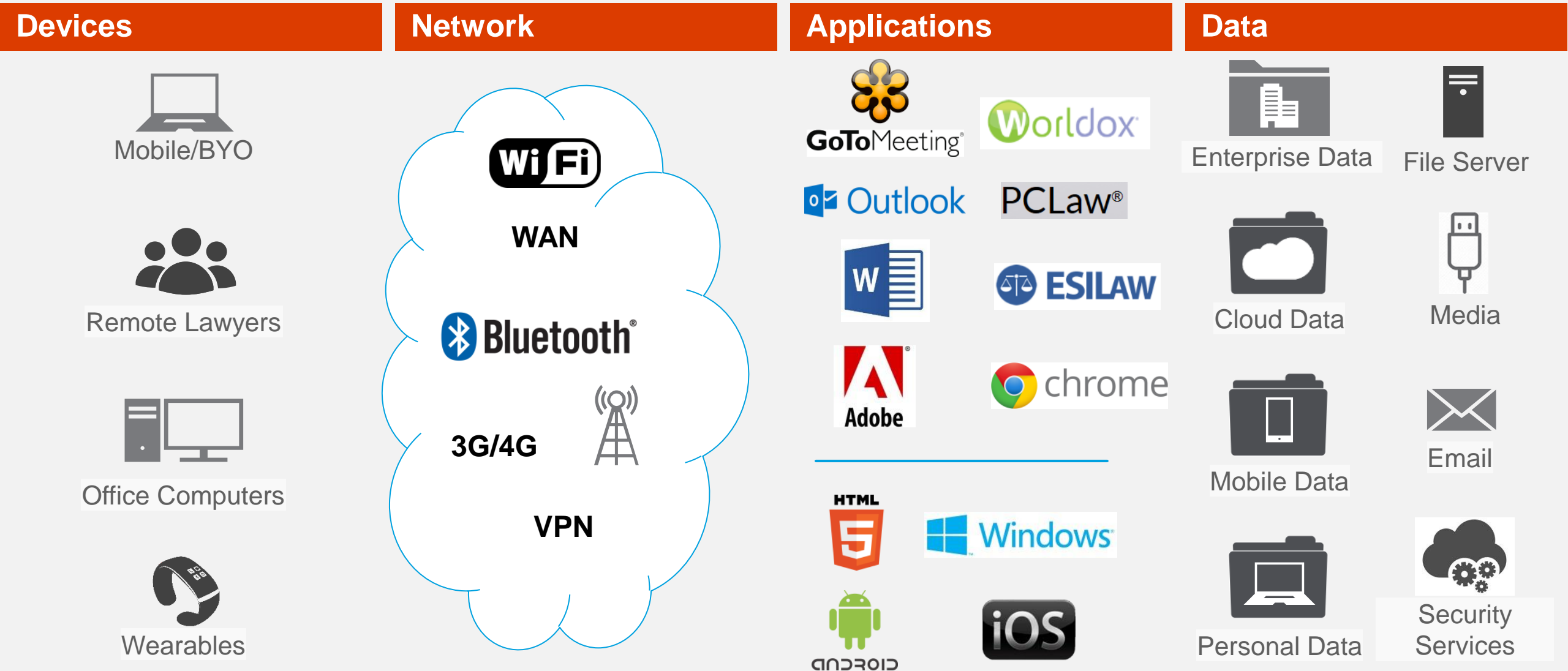


Hacktivists



Criminal Enterprises

Complex IT Requirements



Devices



Mobile/BYO



Remote Lawyers

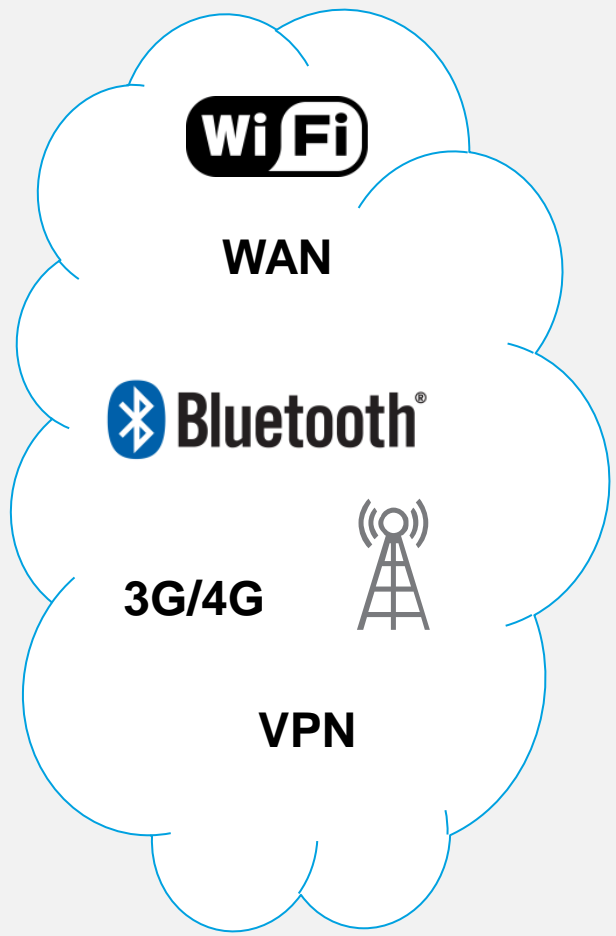


Office Computers



Wearables

Network



Wi-Fi

WAN

Bluetooth

3G/4G



VPN

Applications

GoToMeeting[®] Outlook Word Adobe HTML5 Windows Android iOS Worldox PCLaw[®] ESILAW Chrome

Data

Enterprise Data File Server Cloud Data Media Mobile Data Email Personal Data Security Services

COMMON MYTHS ABOUT THE CLOUD

On-premises is more secure

Data is used for things like advertising

It's not compliant with industry regulations

Control of data in the cloud is lost

THE I-WORX TRUSTED CLOUD...

Built to provide a level of security that exceeds most clients' on-premises infrastructure and scale.

Prohibits the sharing and use of personal data.

Compliant with industry-specific and government regulations.

Designed to give you control of your data. You own it; i-worx manages it for you.

60 %

of business users in the
cloud by 2022¹

\$191B

on cloud computing by
2020²

1. Gartner. "Cloud Office Questions Begin the Shift from 'If' to 'When.'"

2. Forrester. "The Cloud Market Is Now in Hypergrowth."

40%

of employees use a personal device for work¹

4.5M

devices were lost or stolen in 2014²

1. Gartner. "Gartner Says 40 Percent of U.S. Employees of Large Enterprises Use Personally Owned Devices for Work." 2. Consumer Reports. "Smart Phone Theft Rose 3.1 Million in 2013."



MODERN LAW OFFICE

THE I-WORX TRUSTED CLOUD



**DATA CENTRE
INFRASTRUCTURE**



**SECURED DATA AND
COMPLIANCE**



**PROTECTED USERS AND
MANAGED DEVICES**

i-worx Trusted Cloud

Enhanced IT and Security Operations Reduce Risk



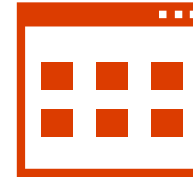
**Identity &
Access**



**Network
Security**

```
101010101010101  
010101010101010  
101010101010101  
010101010101010  
101010101010101  
010101010101010
```

**Data
Security**



**Application
Security**



**Monitoring &
Response**

Confidentiality

Integrity

Availability

i-worx Trusted Cloud

Enhanced IT and Security Operations Reduce Risk



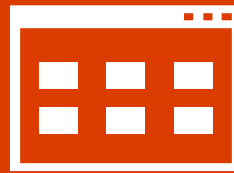
Identity & Access

Authentication
Authorization
Access Control



Network Security

Remote Access
Segmentation
Availability



Application Security

Centralization
Access Control
Inspection



Data Security

Centralization
Containerization
File Sharing



Monitoring & Response

Visibility
Logs
Compliance

Confidentiality

Integrity

Availability



DATA CENTRE INFRASTRUCTURE

Physical Security

Network

Host

Application

Admin

Data

DATA CENTRE LAYERS

Physical Security: 24-hr monitoring, multifactor authentication

Network: Private network

Host (Physical Servers): Limited human interaction

Applications: Secure deployment

Admin: Highly skilled techs, training

Data: Continuous security & encryption investments



DATA CENTRE SECURITY & SERVICES

INCREASE PHYSICAL SECURITY

i-worx's datacenters are protected with safeguards like motion sensors and security breach alarms

ENHANCE YOUR SERVICES

i-worx leverages data centre and network carriers fibers to improve hosted services to clients

A black and white photograph of a man in a polo shirt standing in an office. He is looking down and to the left. In the background, there are several computer monitors on a desk, some displaying data or code. The office has a modern feel with a grid ceiling and large windows.

UPTIME

KEEP SERVICES UP AND RUNNING

You get 99.9% uptime.

A black and white photograph of a man in a dark, long-sleeved button-down shirt looking down at a tablet computer. He is standing in a server room, with server racks and a chain-link fence visible in the background. An orange graphic element is overlaid on the left side of the image, containing the word 'COMPLIANCE' in white capital letters. Below this, a white box contains the text 'PRIVACY OF INFORMATION' and a paragraph about PIPEDA.

COMPLIANCE

PRIVACY OF INFORMATION

Follow the PIPEDA ground rules for handling the privacy of personal information.

A black and white photograph of a woman with dark hair tied back, wearing a striped shirt and a cardigan, standing in a server room. She is looking at a computer monitor and has her hands on a keyboard. The room is filled with rows of server racks, and the lighting is dramatic, with strong highlights and deep shadows.

TRANSPARENCY

KNOW WHERE YOUR DATA IS LOCATED

Your data is stored exclusively in data center's in Canada.

OWNERSHIP OF DATA

Data is owned by you and held by i-worx in escrow.

DATA REPLICATED

DATA REPLICATION AN OPTION FOR YOUR FIRM

Replicate a copy of the data from the cloud to an on premise device.



A black and white photograph of two men in a server room. One man, wearing a zip-up jacket and glasses, is seated at a desk and typing on a keyboard. The other man, wearing a button-down shirt and glasses, stands behind him, looking at the computer monitor. The background shows server racks and network equipment.

PREVENTION

ELIMINATE UNNECESSARY ACCESS

Permissions and access to data is dictated by the client and strictly controlled via policies.

MAINTAIN COMPLETE CONTROL

You must give explicit permission to i-worx to make changes to user accounts and passwords.

A black and white photograph of a woman with long dark hair and bangs, wearing a denim shirt, looking down at her smartphone. She is standing in front of a concrete wall with a window frame visible on the left. The image is partially overlaid by a red and white graphic on the left side.

MOBILE ACCESS

GAIN CONTROL ACROSS DEVICES

Set security policies on user devices.

PROTECT DATA

Secure devices with remote wipes in the event of theft or loss.



SECURE DATA & COMPLIANCE



PRIVACY BY DESIGN

i-worx's Cloud services reside on a private cloud and hence prohibits the sharing of personal data



I-WORX CLOUD SECURITY

RELY ON I-WORX'S INVESTMENTS

i-worx is continuously investing in security software and tools, like advanced ransomware detection.

DEPEND ON TRAINED PERSONNEL

i-worx recruits great talent and invests in our people.

COUNT ON DATA CENTRE'S

Our data centre's has power redundancy, 24/7 monitoring, and advanced physical security.





CLIENT CONTROL

MAINTAIN COMPLETE CONTROL

Granting access and permission to data is controlled by the client

GRANT LIMITED ACCESS

When access is granted to 3rd party vendors, it's given on a just-in-time basis



Clients must provide permission to all data before it can be accessed



A black and white photograph of a modern office interior. The scene is viewed through a glass partition. In the foreground, there's a long, narrow orange banner with the word 'RETENTION' in white. Below it, there are two white boxes containing text. In the background, a man and a woman are sitting at a long, dark conference table. The man is on the left, leaning forward, and the woman is on the right, looking at a laptop. There are several office chairs around the table. Large windows in the background offer a view of a city building.

RETENTION

RETAIN VITAL CONTENT

Save important content with retention policies

EASILY FIND RETAINED CONTENT

Search for and access content as needed for legal and business requirements



DATA PROTECTION

PROTECT DATA ACROSS DEVICES

Set strict controls for users accessing data from different devices

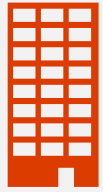
PREVENT DATA LEAKAGE

Keep your data out of the wrong hands with robust policies for protecting email content and documents

LEVERAGE ENCRYPTION

i-worx continuously enhances its encryption capabilities to better safeguard your data

INNOVATIVE CLOUD SERVICES



Infrastructure

Data centres
Physical security
Fiber technologies



Compliance

PIPEDA Standards



Transparency

Local data centers



Prevention

Access controls



Uptime

99.9% uptime



Data replicated

Data copied from cloud to
on premise device

Protected users and managed devices





PEOPLE-CENTRIC APPROACH TO IT

EVERY FIRM

"...has associates who use file sync and share services, whether approved or not."¹

1 to 3

consumer products being used for firm-related tasks²

USER ACCESS MANAGEMENT

MANAGE USER ACCESS

Strict policies are enforced and tools used to manage user access



CLIENT EVIDENCE

CLIENT DATA MORE SECURE IN THE CLOUD

“The move to the cloud brought up all sorts of security questions, and it quickly became clear that our data would be safer in the i-worx private cloud than in our own offices.”

Natalie Foley
Director of Operations
Miller Titerle & Co.

The logo for Miller Titerle & Co. (MT +Co.) is displayed within a white square. The letters 'MT' are stacked above '+Co.' in a bold, white, sans-serif font, all set against a black square background.

CLIENT INFORMATION CONFIDENTIAL

"When we embarked on moving to the cloud, April 2009, one of our primary concerns was ensuring our client's information remained confidential. With i-worx's hosted desktops, we're absolutely satisfied that our data is safe."

Digby Leigh
Managing Partner
Digby Leigh & Company





I-WORX CAN HELP YOUR LAW FIRM ACHIEVE MORE

Learn more and watch the video at www.i-worx.ca

Ready to get started www.i-worx.ca/contact-us

