THE TOP 3 SECURITY THREATS C-LEVEL EXECS NEED TO PREPARE FOR

Impact is imminent. How will your team respond?

ConRes
IT SOLUTIONS

INTRODUCTION

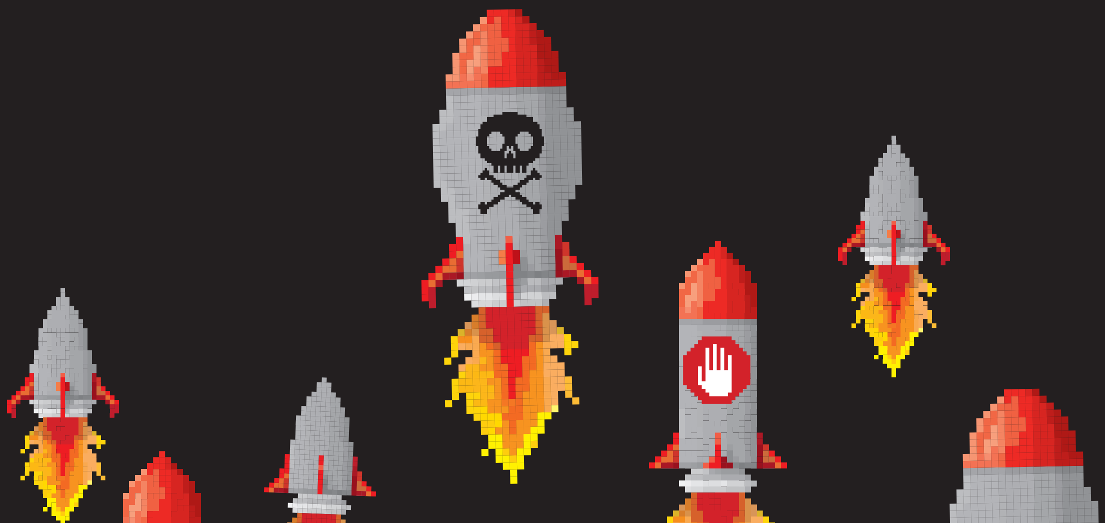
Your company's network is floating through cyberspace. Hacks are heat-seeking missiles built to penetrate and obliterate the defenses surrounding your systems and files. It is no longer a question of if you will be caught in the crossfire. Impact is imminent.

What is your emergency protocol to counteract a network penetration? Do you have an alarm that will sound in the event an end-point is compromised and your data is being secretly stolen away into the unknown?

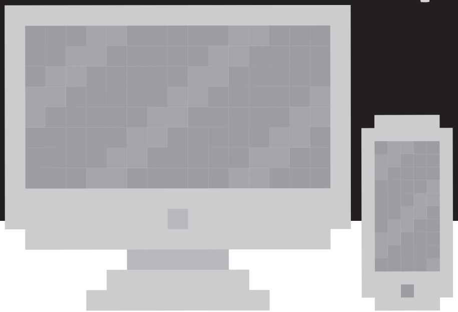
Will your business emerge victorious on this epic cyber battlefield, or will you be made a victim?

Below is a list of three of the latest and greatest security threats that your company is facing off against today.

Plan wisely. Kirk Out.



LEVEL 1:
ENDPOINT AND MOBILE DEVICE MANAGEMENT



Mobile devices are one of the greatest threats against corporate networks today. The Bring Your Own Device (BYOD) issue has sparked great debates at many companies, but the fact is many workers don't understand the security concerns that come with random app downloads. 75% of mobile apps fail basic security tests, for instance.[1] The average large enterprise has around 2,000 unsafe mobile apps installed on employee devices.[2]

App security tops the list of the four greatest enterprise mobility security concerns. Device loss or theft, data leakage, and malware attacks are other serious mobile security concerns. So, how is your business going to bolster data protection? Below are some questions that your IT team needs to consider.

Is your business...

- Utilizing strict BYOD and MDM policies?
- Restricting the download of mobile apps?
- Requiring strong passwords for mobile screen locks?
- Using authentication software?
- Requiring that corporate passwords not be re-used outside of office accounts?
- Checking for malware on personal employee devices that access work files?
- Using anti-malware and anti-virus software that is universal across all brands and platforms?
- Using specialized apps to access and share work data?

1. http://www.gartner.com/newsroom/id/2846017
2. http://www.marketwired.com/press-release/average-large-enterprise-has-more-than-2000-unsafe-mobile-apps-installed-on-employee-1999331.htm

LEVEL 2:
FALLING BEHIND ON COMPLIANCE

With new fees and penalties that are hitting companies that can't remain compliant, the cost of lost or stolen data is mounting for companies of all sizes. By the end of 2014, the average cost of lost or stolen data totaled around $145 per record – a cost that increased more than 9% from 2013.[3] Following compliance regulations has become critical to protecting the data of your employees and clients. How do you stay compliant? And are you at risk of compliance penalty exposure? Here is a checklist of questions that will highlight potential compliance needs. Check out our checklist below.

- ✔ Do your security and risk management groups have access to the most accurate compliance data available?
- ✔ How many access and usage controls do you have over data?
- ✔ Do you have compliance concerns with consumer solutions?
- ✔ Do you have the means to calculate your compliance metrics?
- ✔ Does your operations team have continuous compliance required by security?
- ✔ Do you have automated security configuration management for asset discovery, vulnerability management, and network self-quarantines?
- ✔ Are you able to handle rising security costs?

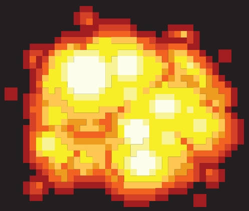
3. http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf

LEVEL 3:
CYBER THREATS

It's not a matter of IF your company will be targeted by cyber threats; it's a matter of WHEN. New cyber-attacks are being designed every second of every day. Bots, designed by brilliant cyber criminals, consistently search to find vulnerabilities in your network and systems, but that's not all you have to protect against. Listed below are the latest cyber-attacks that are wreaking havoc in the digital world.

- **CryptoLocker Attacks** – By breaching servers and then encrypting the data held within, CryptoLocker Attacks hold company information for ransom. The price averages a few hundred dollars per file. Gameover Zeus is one example that has attacked over 1 million computers and cost victims around $100 million dollars total.[4] SMBs are a big target for these types of attacks.
- **Phishing Scams** – As one of the most tricky cyber-attacks out there, phishing emails are meticulously crafted by malevolent cyber-criminals – all for the purpose of getting users to click links that will seize information. In 2014, Google announced that it had detected 90,000 phishing sites and 50,000 infected sites.[5]
- **Distributed Denial-of-Service Attacks** – These attacks are on the rise in the enterprise, as they shut down online services with overwhelming amounts of traffic. Downtimes lead to chaos, and in the process of booting back up and discovering what went wrong, information – like customer data or intellectual property – is typically spirited away by cybercriminals.[6]
- **Attack-as-a-Service** – As a new form of attack expected to take off in 2015, Attack-as-a-Service will allow malevolent buyers to "visit a website, select a malware platform, and choose targeted information, such as bank records and credit cards."[7] Because this is a newly growing threat, it is still uncertain what impact this form of attack will have on the security world.

[4] *http://www.news8000.com/us-puts-reward-out-for-russian-web-criminal/31454074*
[5] *http://googleblog.blogspot.com/2015/03/protecting-people-across-web-with.html*
[6] *http://www.zdnet.com/article/ddos-attacks-costs-enterprise-100000-per-hour-study-finds/*
[7] *http://www.zdnet.com/article/the-state-of-cybersecurity-in-the-enterprise-in-2015/*



CONCLUSION

Overall, companies need to unify their security tactics and fortify network protection to prepare for the newest onslaught of threats that are armed, dangerous, and devastating to companies that do nothing.

The moral of the story: Arm your business to ensure the longevity of your operations and fight back against the malevolent, malicious evil-doers.

Discover the latest tools your company can use to fortify your defenses against incoming attacks. Reach out to a ConRes expert today to craft a one-of-a-kind battle strategy.

ConRes IT SOLUTIONS

Premier Business Partner IBM