IS YOUR BUSINESS SAFE FROM HACKERS IN 2017

SECURITY THREATS

CYBER ATTACKS ARE ON THE RISE

In 2017 we have seen an unprecedented amount of large-scale cyber attacks. With the CIA Vault 7 data leak, the pre-election Macron e-mail hack, and the enormous Petya ransomware attack that crippled major businesses across 14 different countries - to name a few, the trend seems evident with no signs of slowing down.

But, it's not just financial damage that is caused by these attacks. The reputations of businesses suffer with each incident. In spite of this, businesses widely admit that they are ill prepared to deal with cyber threats of any kind.

You need to learn how to effectively take precautions and combat cyber attacks before they occur. Investing in the protection of customer data and building solid intrusion detection systems are key to a successful cyber defense strategy.

Cyber attacks are becoming more severe and more frequent

75% THE SEVERITY OF ATTACKS IS ON THE RISE

68% THE FREQUENCY OF ATTACKS IS ON THE RISE

53% LAUNCHING A STRONG OFFENSIVE AGAINST HACKERS IS IMPORTANT

46% OUR ORGANIZATION IS VIGILANT IN MONITORING ATTACKS

27% OUR SECURITY BUDGET IS SUFFICIENT FOR MITIGATING MOST ATTACKS

Source: Ponemon Institute, strongly agree and agree responses combined

Public scrutiny / bad publicity can harm businesses of any size

PUBLIC SCRUTINY

SOURCE: CISCO SURVEY

54% of organisations responding to Cisco's security capabilities benchmark study had to manage public scrutiny after a data security breach.

BAD PUBLICITY

SOURCE: PWC REPORT

After the worst security incident of the year, 17% of organizations suffered extensive adverse media coverage over a prolonged period.

Businesses fear reputation damage due to breaches most

WHAT MADE A PARTICULAR INCIDENT THE WORST OF THE YEAR?

42% REPUTATIONAL DAMAGE

23% BUSINESS DISRUPTION

15% INVESTIGATE & FIX COST

10% VALUE OF LOST ASSETS

10% OTHER FACTORS

Source: PWC

Investing in protecting customer data can mitigate that

WHAT IS THE MAIN DRIVER FOR INFORMATION SECURITY?

34% PROTECTING CUSTOMER DATA

21% PROTECTING REPUTATION

11% PREVENT DOWNTIME & OUTAGES

10% PROTECTING IP

10% COMPLYING WITH LAWS / REGULATIONS

5% MAINTAINING DATA INTEGRITY

Source: PWC

So what can businesses do?

DETECTION IS KING

BE PREPARED TO DETECT

The longer an attacker is inside your network, the greater the damage they can cause. The most severe attacks are often the ones that go undetected for days or even weeks. Intrusion detection systems and a good analytics setup with 24h notifications can go a long way in reacting to the next system intrusion in time.

REACTION SAVES THE DAY

BE PREPARED TO REACT QUICKLY

Make sure you have access to experienced cyber security experts who are familiar with your IT infrastructure and setup. If you are running a small business without an IT department you can outsource this to a range of different IT service providers, who can step in when needed.

Is investing in cyber security software the answer?

YES (BUT)...

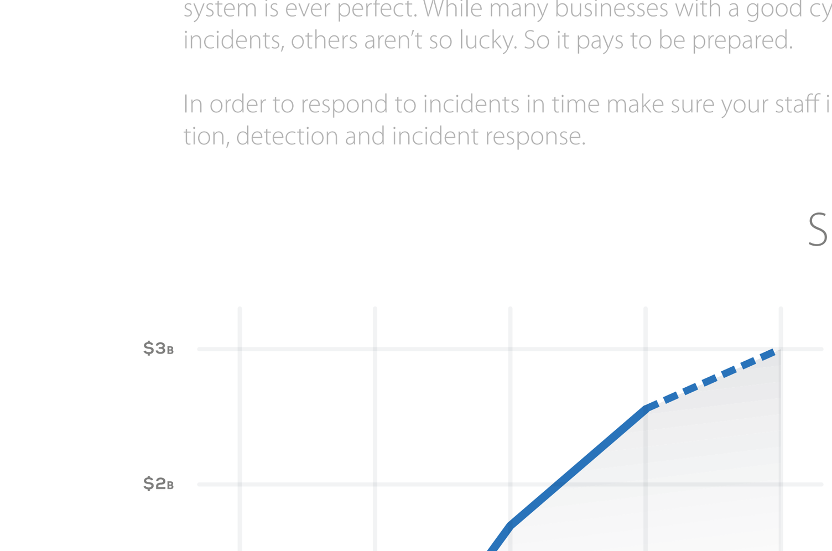
IT'S JUST A PIECE OF THE PUZZLE

According to the SANS Institute 66% of businesses blame staff and skills shortages as the core impediments to timely cyber incident response. Software can significantly improve your business's detection and prevention setup, but no system is ever perfect. While many businesses with a good cyber security setup manage to get by for years without major incidents, others aren't so lucky. So it pays to be prepared.

In order to respond to incidents in time make sure your staff is trained in using cyber security software, as well as prevention, detection and incident response.

SECURITY SOFTWARE AVAILABILITY

Funding in cyber and cloud security software companies has nearly doubled over the last 2 years. Additionally, a lot of the previous years' investment is resulting in a recent surge in new cyber security technology types. Crozdesk has found that the variety of new IT security (and related) software solutions launched onto the market has increased by nearly 350% from June 2016 to June 2017, as compared to the 12 months period before.



Funding raised by cyber and cloud security businesses. Source: Crozdesk and Crunchbase data (2017 projection)

+350% NEW IT SECURITY SOFTWARE INTRODUCTIONS

From Jul 2016 - Jun 2017, as compared to Jul 2015 - Jun 2016
Source: Crozdesk data

What software do you need? The checklist!

SECURING YOUR NETWORK...

A QUICK OVERVIEW OF WHAT TECHNOLOGIES ARE OUT THERE

The checklist below will show you the network security technologies businesses with more than 500 employees are using or are planning to add to their stack. Honeypots (traps for intruders) are on top of the wish list for 2017.

Whether your business is big or small, have a close look at the technologies below and consider adding applicable ones to your cyber security setup.

NETWORK SECURITY TECHNOLOGIES USED OR PLANNED FOR ACQUISITION IN 2017

	CURRENT	PLANNED
NETWORK-BASED ANTIVIRUS	68%	25%
ADVANCED MALWARE ANALYSIS / SANDBOXING	67%	24%
SECURE EMAIL GATEWAY	63%	26%
SECURE WEB GATEWAY	62%	26%
WEB APPLICATION FIREWALL	62%	29%
INTRUSION DETECTION / PREVENTION SYSTEM	59%	30%
DATA LOSS / LEAK PREVENTION	57%	35%
DENIAL OF SERVICE (DOS/DDOS) PREVENTION	56%	30%
SECURITY INFORMATION AND EVENT MANAGEMENT	55%	33%
SECURITY ANALYTICS / FULL-PACKET CAPTURE AND ANALYSIS	52%	35%
PRIVILEGED ACCOUNT / ACCESS MANAGEMENT	52%	33%
NETWORK BEHAVIOR ANALYSIS / NETFLOW ANALYSIS	51%	34%
NEXT-GENERATION FIREWALL	48%	39%
THREAT INTELLIGENCE SERVICE	46%	37%
USER AND ENTITY BEHAVIOR ANALYTICS	45%	38%
HONEYPOTS / NETWORK DECEPTION	35%	41%

Bavased on 1,100 responses from companies with >500 employees across 15 different countries
Source: CyberEdge Group

READ THE FULL REPORT ON CROZDESK.COM

DESIGNED BY crozdesk™ business software search

Based on the report 'How to raise your organisation's security maturity level' by Bloor Senior Software Analyst Fran Howarth.
Some data has been updated and new data has been included. The full report is available here:
https://crozdesk.com/software-research/how-to-raise-your-organisation-s-security-maturity-level

PUBLISHED IN COLLABORATION WITH

CYBERSPARTA

We believe even the most daunting challenges can be overcome through team work and partnerships. In building the ATHENA Cyber Platform, we envisaged a future-proofed cyber solution 10x more effective than existing options. The result? Improved security and ROI throughout the organisational cyber security chain. CyberSparta was established in 2016 by an international team of cyber, Big Data science and business professionals. We are headquartered in the UK.

web www.cybersparta.com **twitter** @Cybersparta
email theteam@cybersparta.com

CYBERQ GROUP

To Face the cyber challenge head on you need , collaboration, innovative technology and great people. We are bringing together the best of all those components, keeping your business better protected. Which means an Improved business risk profile, significant operational cost savings and long term peace of mind.

web www.cyberqgroup.com **twitter** @cyberq_group
email info@cyberqgroup.com