



## BACK TO BASICS PER LA CYBERSECURITY

WEBINAR 15 Aprile 2020- dalle 11.30 alle 12.30



F-Secure



# Back to Basics per la Cybersecurity

Misure e risposte concrete per mettere in sicurezza persone e processi

WEBINAR 15 aprile 2020



# AGENDA

*Molte aziende si pongono oggi la domanda: cosa non deve mancare nel mio Piano di Cybersecurity? quali sono le misure e i processi prioritari da prevedere, per*

- *Proteggere una forza lavoro che, in questo momento, si collega in massa dalla propria abitazione*
- *Sostenere un traffico più elevato, rispondere con tempestività in caso di attacco cyber*
- *Sensibilizzare le persone, formarle per uno Smart Working in sicurezza*
- *Riposizionare la difesa tenendo conto della continua evoluzione delle minacce.*

I temi saranno affrontati nel Webinar di oggi con

- 11:30 – 11.40      **Elena Vaciago**, Associate Research Manager di **The Innovation Group**
- 11.40 – 11.50      **Corradino Corradi**, Head of ICT Security & Fraud Management di **Vodafone**
- 11.50 – 12.00      **Andrea Muzzi**, Technical Manager di **F-Secure**
- 12.00 – 12.10      **Paolo Arcagni**, Manager, System Engineering Italy & Iberia di **F5 Networks**
- 12:10 – 12:20      **Stefano Ricci**, Senior Sales Engineer di **Rubrik**
- 12:20 – 12:30      **Domande & Risposte**

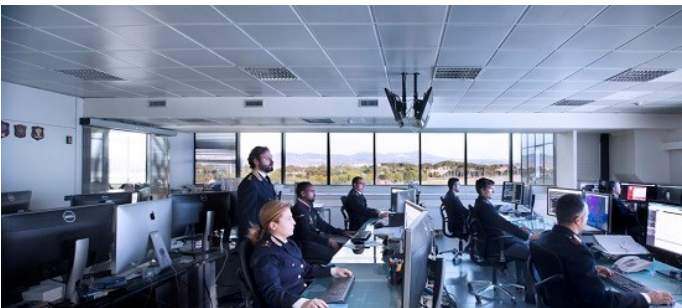
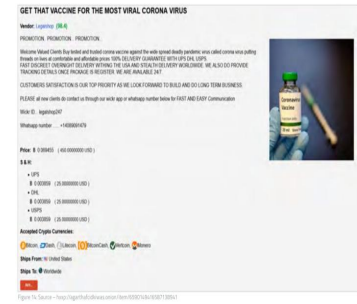
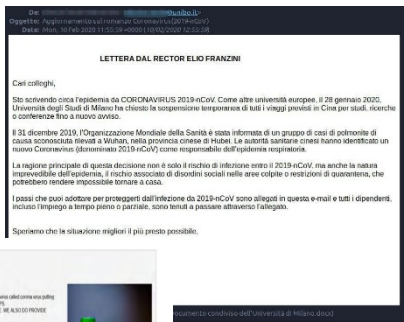
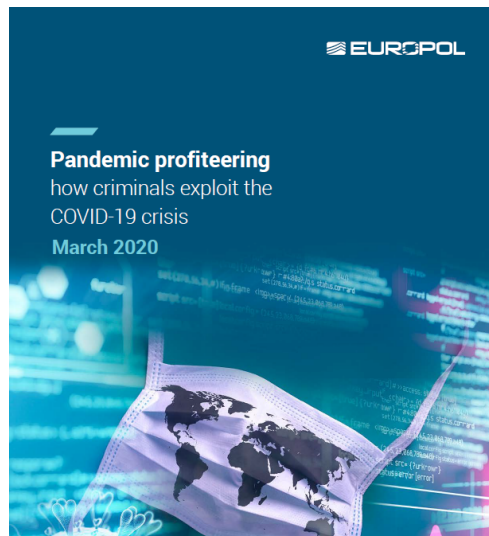


**#TIGcybersec**

[channels.theinnovationgroup.it/cybersecurity](https://channels.theinnovationgroup.it/cybersecurity)



# ALERT: crescita dei Rischi Cyber nei giorni dell'epidemia da Covid-19

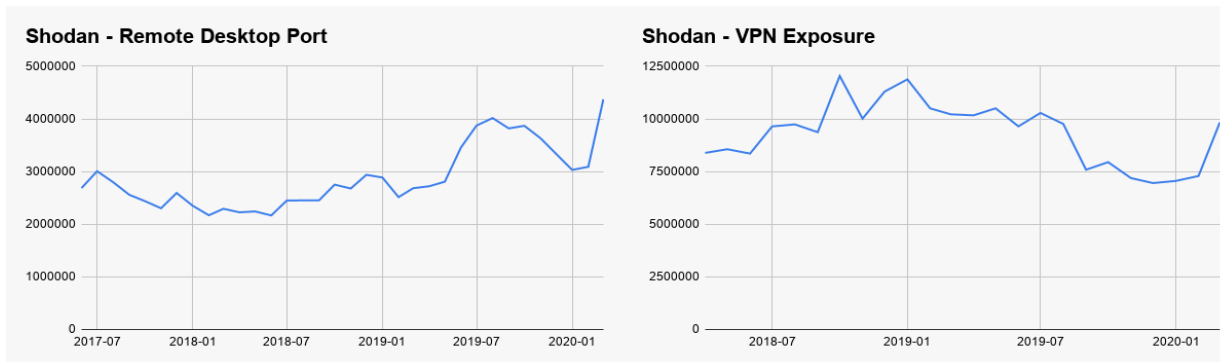




# Ripensare la Resilienza con una forza di lavoro distribuita

Utilizzo di RDP in crescita del 41%, utilizzo di Enterprise VPN del 33%  
nelle due settimane centrali di marzo 2020

MAGGIORE  
DOMANDA  
DI SICUREZZA



NUOVI  
RISCHI ...



VECCHI  
PROBLEMI ... **Smart working e didattica online? Ma il 33% delle famiglie non ha pc o tablet a casa**

REPORT

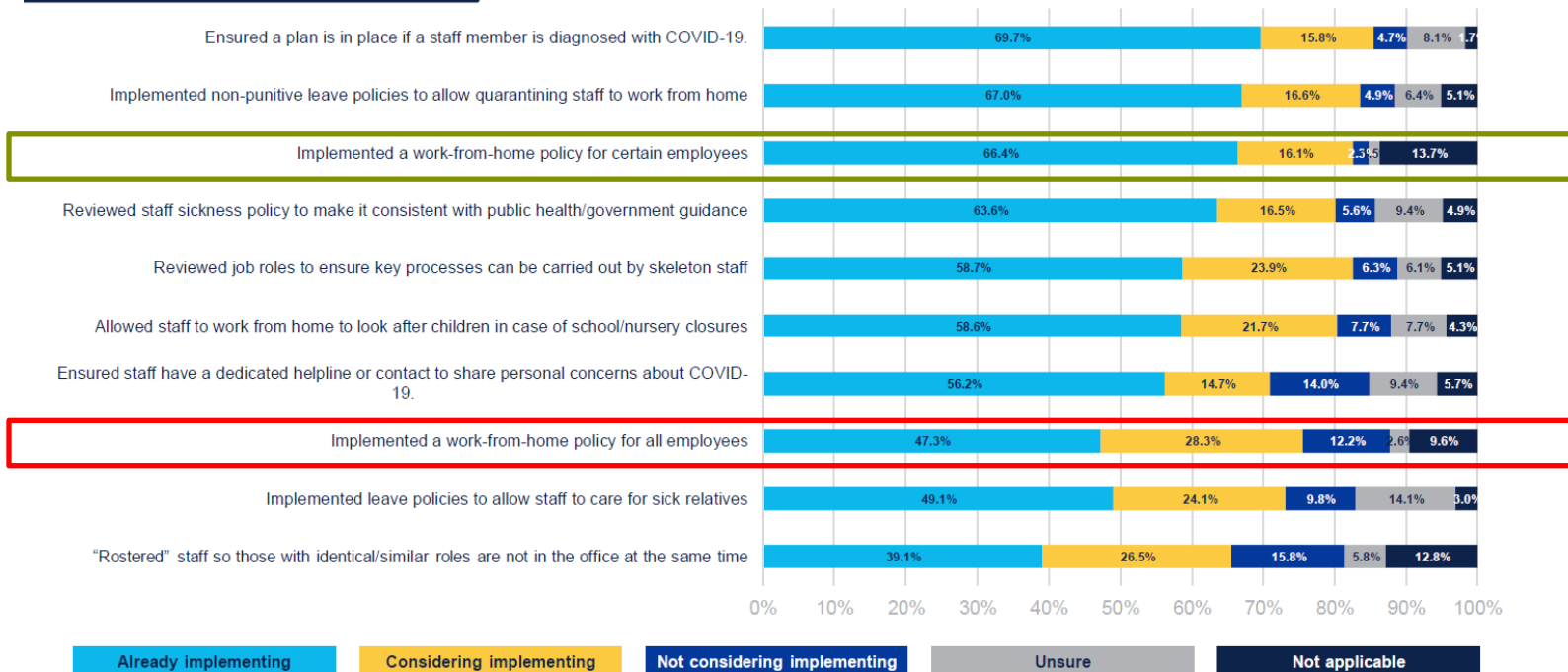
di Paolo Anastasio | 6 Aprile 2020, ore 14:45



# Come affrontare l'emergenza e garantire la continuità?...

**bci** Leading the way  
to resilience

Which of the following HR and staff measures have you taken or are considering taking in your organization?



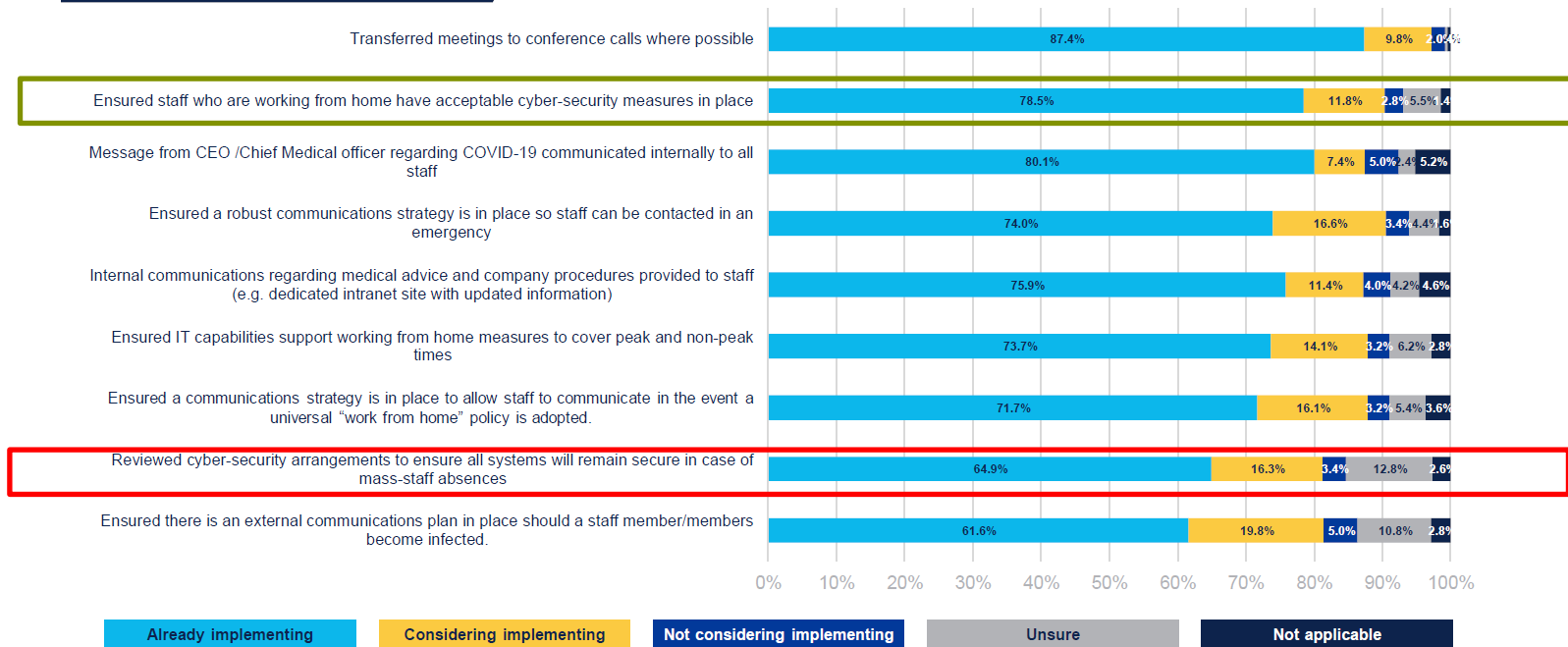
4 [www.thebci.org](http://www.thebci.org)



# ... e quali sono le misure da prevedere per la Cybersecurity?

**bci** Leading the way  
to resilience

Which of the following IT, technology and communications measures have you taken or are considering taking in your organization?

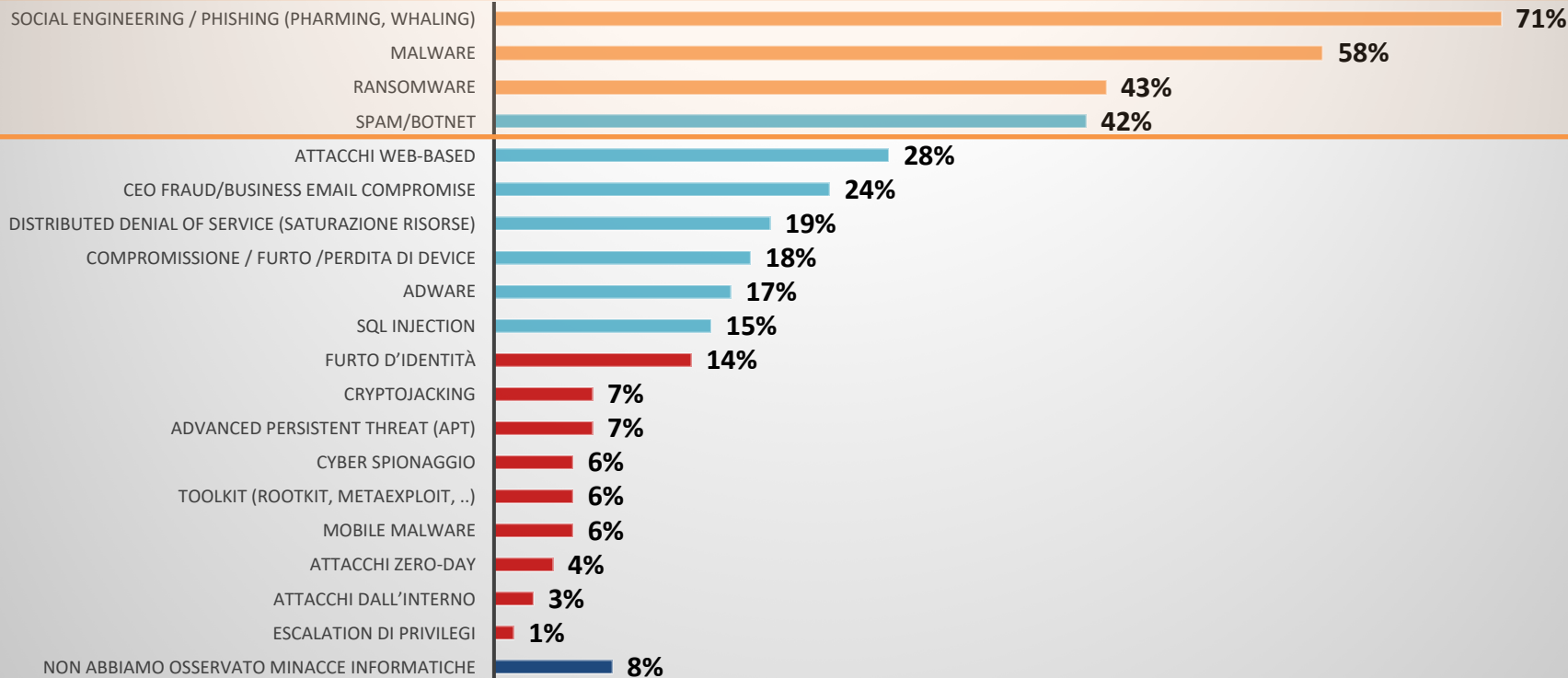


10 [www.thebci.org](http://www.thebci.org)



# Il Phishing è oggi la minaccia cyber osservata con maggiore frequenza, seguita da malware, ransomware, spam

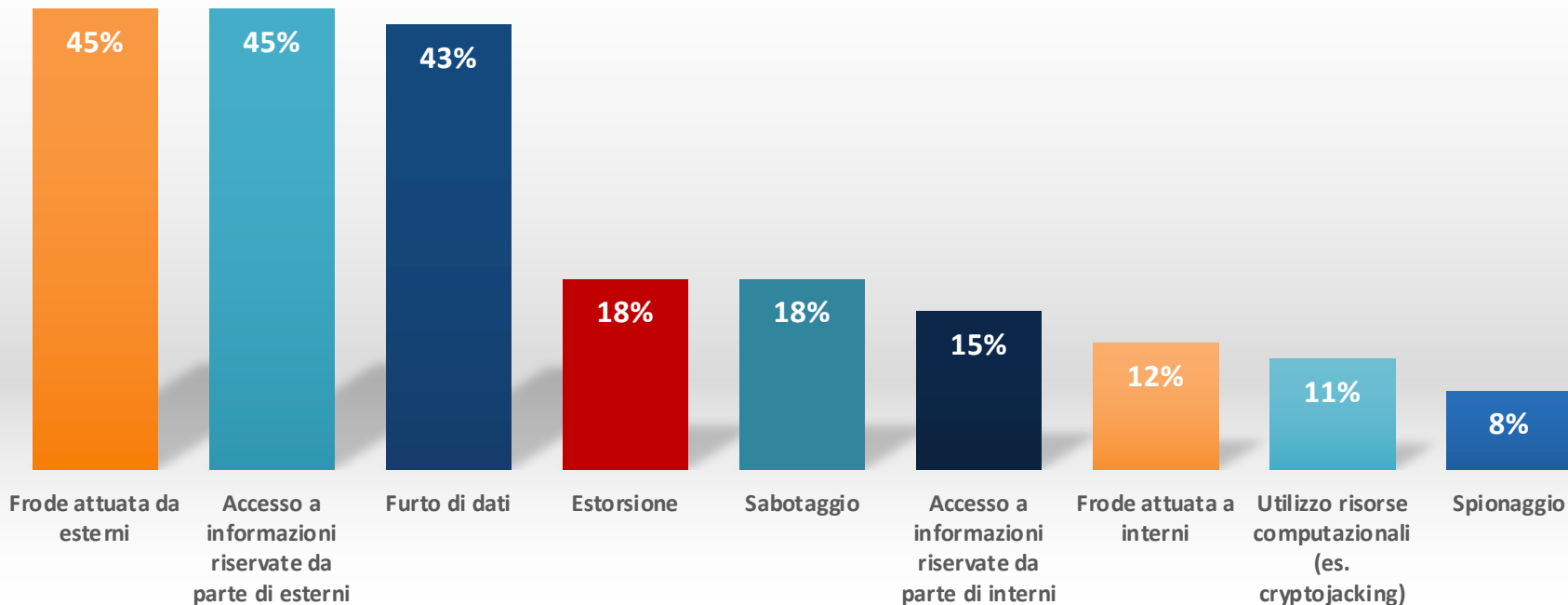
Nel corso degli ultimi 12 mesi, quali dei seguenti attacchi cyber hanno riguardato la Sua azienda?





# Le motivazioni che spingono il cyber crime sono molteplici, ma prevalgono nettamente quelle a scopo economico

Quali erano le finalità degli attacchi osservati?

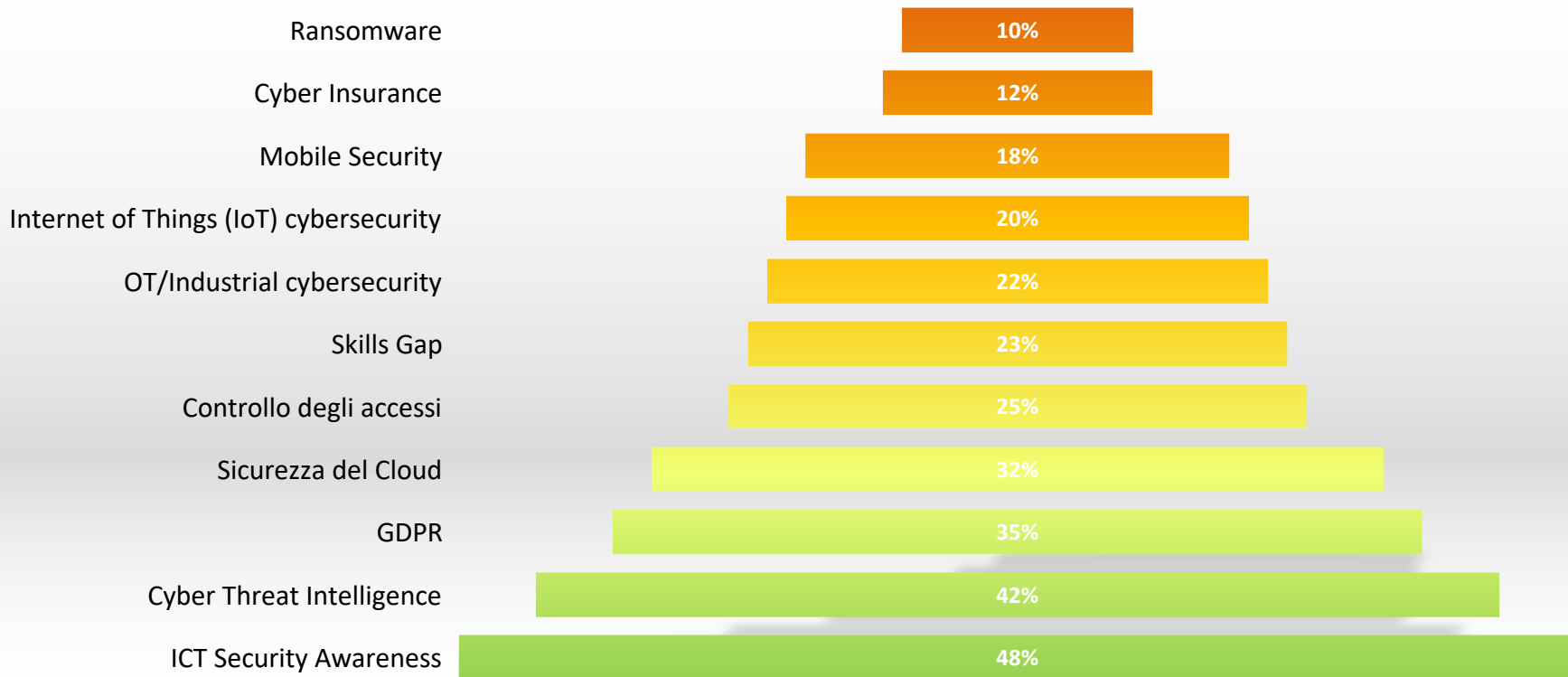






# Spostamento di focus sui temi del Fattore Umano e dell'Intelligence

Quali dei seguenti Hot Topic sono secondo Lei oggi più rilevanti per un CISO/Security Manager?





# Back to Basics: facciamo ordine sui «fondamentali» per la cybersecurity



## Stay Safe Online Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand why you might be vulnerable to cyber attack, and how to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

## SAFE TELEWORKING

### FOR BUSINESSES

Establish corporate policies and procedures



Secure your teleworking equipment



Provide secure remote access



Keep device operating systems and apps updated



Secure your corporate communications



Increase your security monitoring



Raise staff awareness about the risks of teleworking



Regularly check in with the staff



### FOR EMPLOYEES

Access company data with corporate equipment



Use secure remote access



Keep business and leisure apart



Avoid giving out personal information



Be careful when using private devices for telework



Think before connecting



Protect your teleworking equipment and environment



Stay alert



Develop new routines



Report suspicious activity



### Who is behind cyber attacks?

#### Online criminals

Are really good at identifying what can be needed for a remote working or selling sensitive data, or holding systems and information to ransom.



#### Foreign governments

Increasingly interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.



#### Hackers

Individuals with varying degrees of expertise, often acting for an unknown reason - perhaps to test their own skills or cause disruption for the sake of it.



#### Political activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.



#### Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.



#### Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity such as using sensitive information to share with young competitors.



#### Honest mistakes

Sometimes staff, with the best of intentions, just make a mistake, for example by emailing something sensitive to the wrong email address.



© Crown Copyright 2018

### Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try to trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.

Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings, and think about what you post.

Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.

Phishers often seek to exploit 'normal' business communications and processes. Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.

Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.

Secure your devices

The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.

Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.

Always lock your device when you're not using it. Use a PIN, password, or fingerprint ID. This will make it harder for an attacker to exploit a device if it is left unattended, lost or stolen.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.

If you write your passwords down, store them securely away from your device. Never reveal your password to anyone, not your IT team or other provider who will be able to reset it if necessary.

Use two factor authentication (2FA) for important activities like banking and email. If you're given the option, 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

Reporting incidents promptly - usually to your IT team or line manager - can massively reduce the potential harm caused by cyber incidents.

Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicking on a bad link), always report what's happened.

Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.

www.ncsc.gov.uk @ncsc National Cyber Security Centre

## Seven Imperatives to Protect Against Cyber Risks During the COVID-19 Crisis

As companies ask millions of staff to work remotely from home, they must take the following steps to safeguard their IT systems and data from cyber attack:

- 1 Assess core IT infrastructure for remote working
- 2 Secure applications and devices for the remote workforce
- 3 Embed cybersecurity into business continuity plans
- 4 Make the newly remote workforce aware of the added security risks
- 5 Establish protocols and behaviors to prepare for secure remote working
- 6 Embed cybersecurity in corporate crisis management
- 7 Update access and security measures

Source: BCG analysis.



## *I prossimi appuntamenti TIG: STAY TUNED!!*



### **WEBINAR: SMARTWORKING E CYBERSECURITY**

**06.05.2020** – ONLINE dalle 15.00  
alle 16.00



### **CYBERSECURITY SUMMIT ROMA 2020**

**02.07.2020** - Centro Congressi  
Roma Eventi Fontana di Trevi –  
Roma



# GRAZIE PER LA PARTECIPAZIONE!