The security problem of John’s “other” laptop

How to keep your organization’s data safe during the Work From Home evolution

BeckITSystems® Inc.

Love it or hate it, Working From Home is huge and here to stay.

As a nation, we've really embraced the changes forced upon us by the pandemic. Many businesses have become more flexible with a mixture of office-based workers, hybrid workers, and fully remote workers.

We had no idea that we could change so much, so quickly, did we? Work just doesn't look the same as it did in 2019.

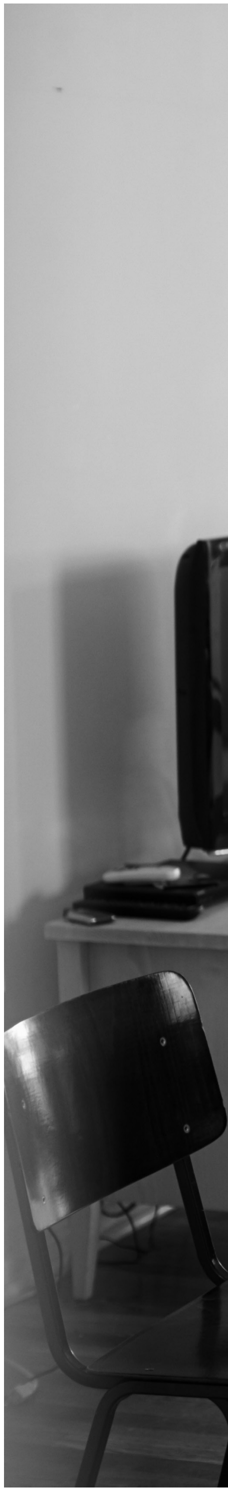
And because of that, cyber security in 2022 doesn't look the same either. When you have people working away from your office you need to take additional security measures to keep your data safe.

Even before we heard the word "Coronavirus", many of us were working from home now and then. Checking emails over the weekend. Finishing up a project in the evening. Getting a head start on the new week.

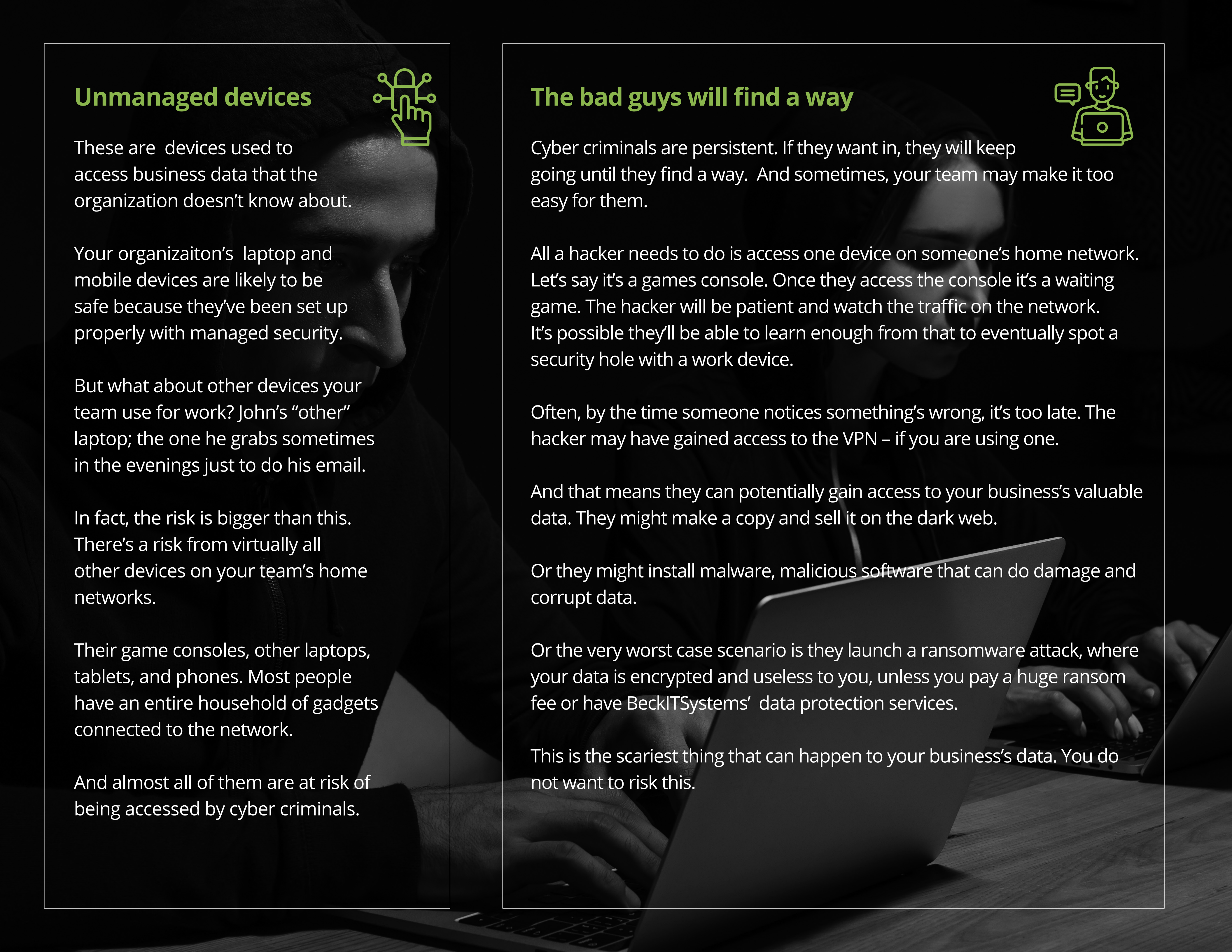
Now Working From Home has to be taken more seriously. If anyone works anywhere away from the office, there's a chance they may take unnecessary risks with data.

Many businesses seem to have this covered. They've invested in new company devices, increased remote security, and have trained their people on best practices.

But there's something important some oragnizations haven't considered.



Working From Home is huge **and here to stay.**



Unmanaged devices

These are devices used to access business data that the organization doesn't know about.

Your organizaiton's laptop and mobile devices are likely to be safe because they've been set up properly with managed security.

But what about other devices your team use for work? John's "other" laptop; the one he grabs sometimes in the evenings just to do his email.

In fact, the risk is bigger than this. There's a risk from virtually all other devices on your team's home networks.

Their game consoles, other laptops, tablets, and phones. Most people have an entire household of gadgets connected to the network.

And almost all of them are at risk of being accessed by cyber criminals.

The bad guys will find a way

Cyber criminals are persistent. If they want in, they will keep going until they find a way. And sometimes, your team may make it too easy for them.

All a hacker needs to do is access one device on someone's home network. Let's say it's a games console. Once they access the console it's a waiting game. The hacker will be patient and watch the traffic on the network. It's possible they'll be able to learn enough from that to eventually spot a security hole with a work device.

Often, by the time someone notices something's wrong, it's too late. The hacker may have gained access to the VPN – if you are using one.

And that means they can potentially gain access to your business's valuable data. They might make a copy and sell it on the dark web.

Or they might install malware, malicious software that can do damage and corrupt data.

Or the very worst case scenario is they launch a ransomware attack, where your data is encrypted and useless to you, unless you pay a huge ransom fee or have BeckITSystems' data protection services.

This is the scariest thing that can happen to your business's data. You do not want to risk this.

What's the **solution?**

The answer isn't straightforward. Unless your business wants to take on the security responsibility of all of your staff's home networks, and all of their devices too.

That's just not realistic.

However, there are things you can do to reduce the risk of an intruder getting into your business network through an unsecured home network. And it all comes down to a layered approach to security.

There are five things we recommend.

Help your team secure their home routers

The router is the box that spreads the internet around the house. You might know it as the Wi-Fi box.

You can give every member of your team advice and direct support keeping their router secure.

Things like changing default administrator passwords are extremely important strategies.

Making sure the router's operating system, known as firmware, is always up-to-date.

Disabling remote access to the Internet router, so no-one can change anything in the router unless they are physically connected to the router.

You could create a policy to make it clear your team must follow standard security guidance for their home network if they want to Work From Home.

01

Make sure your systems are monitored

Your IT support partner should be monitoring your systems. That doesn't mean having a quick check that everything is working as it should be, and waiting for alerts to any issues.

It means they should monitor your network components 24/7, looking for anything unusual that may cause an issue. And preventing problems from escalating.

Unfortunately, cyber criminals don't work to our schedules. They certainly don't work a 9-5 job. It's more likely that they'll make changes when they believe no-one is watching.

And they may launch an attack on a Sunday morning to give them as much time as possible to do what they want to do.

02

Reassess your VPN

Virtual Private Networks have been tools in use over the last couple of years. But while they can allow remote access to your business network, the large-scale use of VPNs has actually created a higher risk of a data breach.

If a hacker breached a device using a VPN to get onto your network, it means they could have full access to everything... without needing to pass further security measures. In addition, a VPN does NOT protect any computer or network from malware infections!

VPNs mainly cloak your Internet address and make it possible to watch Netflix from locations outside of the US. -- **That's scary!!**

An alternative is to remove the VPN, if you have one, and take a zero-trust approach.

This means the credentials of every device and person trying to access the network is challenged and must be confirmed. In that case, if someone gains access, they can only cause damage to the specific system they have accessed.

Create a BCP

A Business Continuity Plan (BCP) helps organizaiton to continue critical business functions in the event of an unplanned event, whether caused by natural events, human errors, or cyber-security attacks. It outlines instructions and procedures an organization can follow. Your BCP will be more comprehensive than a disaster recovery plan (DRP) because a DRP mainly focuses on recovering from disruptions in IT infrastructures. A business continuity plan contains strategies for overconing the effects of additional issues including business processes, organizational assets, leadership changes, software applications and more.

When developing your BCP, there are many things for which to plan. If a disaster took place, is there a tested strategy to quickly restorer each of these functions: the human resources, sales, operations to prevent revenue loss? A business continuity plan needs to provide a framework for recovering from multiple threats.

Beghinning in March of 2022, BeckITSystems will provide BCP planning by Zoom meeting for small organizaitons that want to have a written BCP ready to go. Contact us.

Trust a true partner to worry about this for you

Are you 100% happy with your current IT support provider?

Your technology strategy is too important to be trusted to a company you don’t have a true partnership with.

We’re now taking on a limited number of new clients.
Get in touch and let’s have a short no obligation conversation about your business.

CALL: 703-433-0732 | EMAIL: Ask@BeckITSystems.com
WEBSITE: https://www.beckitsystems.com

BeckITSystems®
Inc.