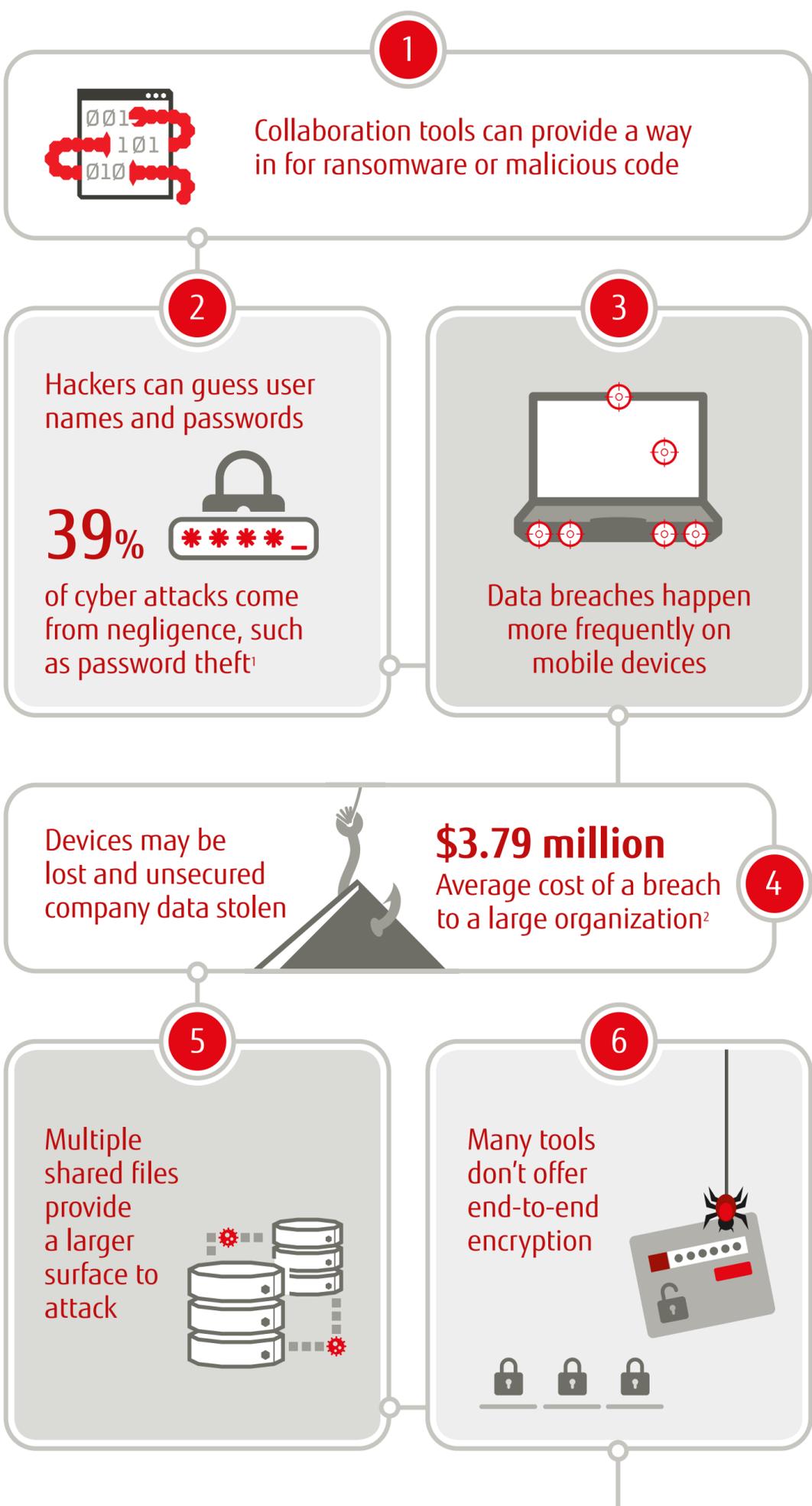FUJITSU

The importance of secure collaboration in the future workplace

Collaboration tools are crucial. When people work together, they can solve problems and innovate quicker. But without the right security, could these same tools also put your organization at risk?

1

001
101
010

Collaboration tools can provide a way in for ransomware or malicious code

2

Hackers can guess user names and passwords

39%

****_

of cyber attacks come from negligence, such as password theft[1]

3

Data breaches happen more frequently on mobile devices

Devices may be lost and unsecured company data stolen

$3.79 million

Average cost of a breach to a large organization[2]

4

5

Multiple shared files provide a larger surface to attack

6

Many tools don't offer end-to-end encryption

So, how do you respond?

Act now: prepare for secure collaboration

1 **Run a risk assessment**
Find out where your weak points are in advance.

2 **Understand how your employees need to collaborate**
Match access to people's job roles.
And use secure digital tools to work with external partners.

3 **Create an enterprise collaboration security policy**
Lay down ground rules for employee behavior to keep your business safe.

4 **Think end-to-end**
From mobile device updates to virtual or on-premise data centers - have the right ecosystem in place.

5 **Develop a training plan**
Have training and best practices in place before your tools go live.

6 **Build a secure enterprise sync and share system**
This will help you monitor usage patterns, detect anomalies, and wipe data if a device is lost or stolen.

7 **Create smart and secure meeting spaces**
Get started and get secure, with a wireless presentation system.

8 **Keep security as a priority**
Regularly reviewing your collaboration practices will help you stay one step ahead of the threats.

Always make security a priority when you're weighing up your collaboration options.

Read more at www.fujitsu.com/global/microsite/workplace

FUJITSU