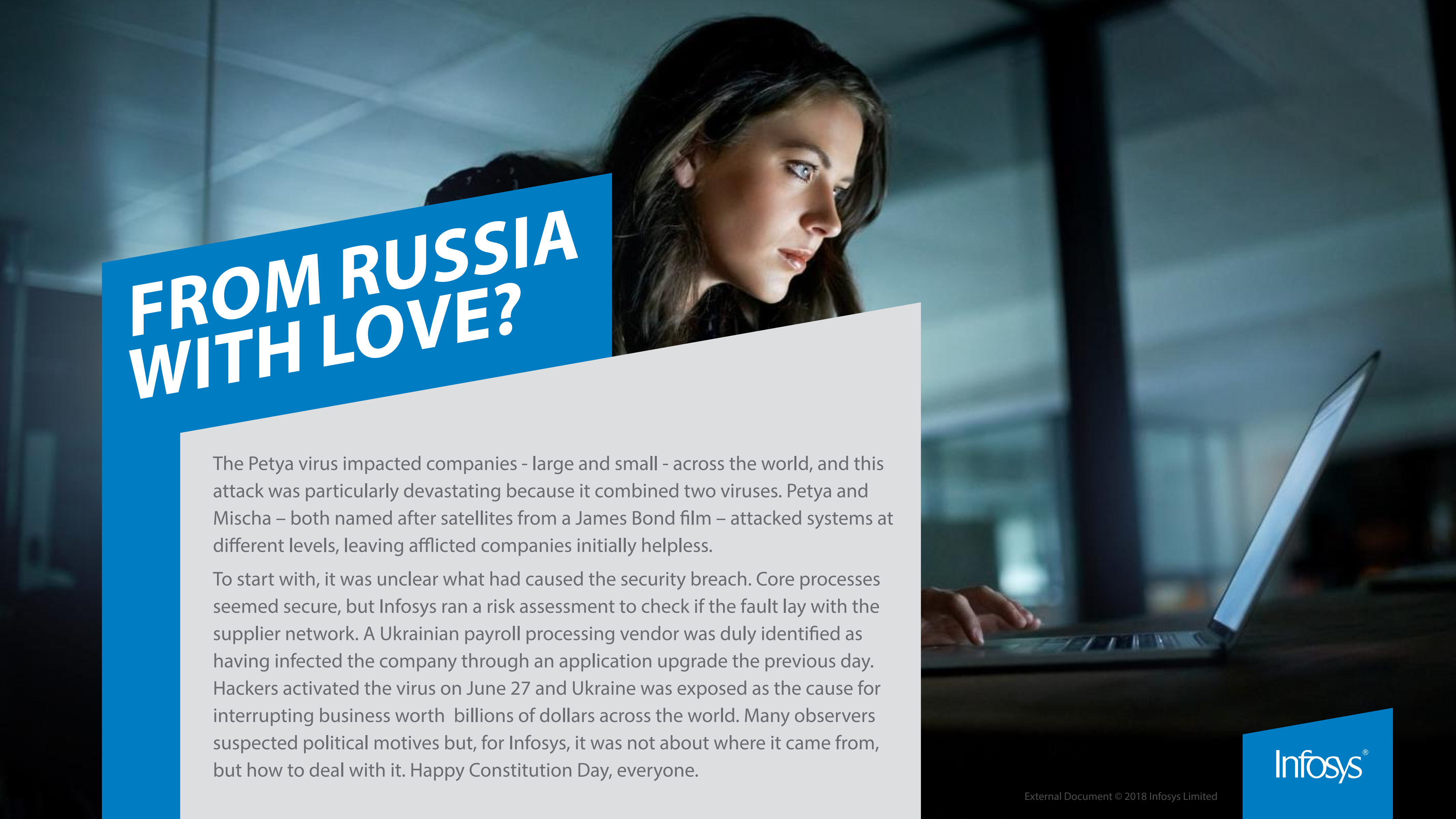
UKRAINIAN CONSTITUTION DAY, PETYA, AND GLOBAL PANIC

HOW ONE COMPANY ENSURED IT WILL NEVER BE IMPACTED IN THE SAME WAY BY MALWARE

June 28 is Ukrainian Constitution Day. It is also one of the longer days of the year – and in 2017, for the staff at one multinational corporation, it certainly felt that way. They arrived at work to find computers locked by the Petya ransomware. Would the company grind to a halt? Would they be held to ransom? How could they prevent it from happening again?

These were the questions. Infosys was hired to provide the answers.

Infosys®



FROM RUSSIA WITH LOVE?

The Petya virus impacted companies - large and small - across the world, and this attack was particularly devastating because it combined two viruses. Petya and Mischa – both named after satellites from a James Bond film – attacked systems at different levels, leaving afflicted companies initially helpless.

To start with, it was unclear what had caused the security breach. Core processes seemed secure, but Infosys ran a risk assessment to check if the fault lay with the supplier network. A Ukrainian payroll processing vendor was duly identified as having infected the company through an application upgrade the previous day. Hackers activated the virus on June 27 and Ukraine was exposed as the cause for interrupting business worth billions of dollars across the world. Many observers suspected political motives but, for Infosys, it was not about where it came from, but how to deal with it. Happy Constitution Day, everyone.

READY TO DEFEND

Having worked out how it happened, the task was now to address the problem. The systems had to be restored as quickly as possible and it had to be ensured that the company was better protected next time.

This was a key breakthrough for Infosys and their client. Viruses and malware are changing constantly, and defenses will occasionally be breached. In the ongoing war between malware perpetrators and cyber-security defenses, some battles will, inevitably, be lost. The smartest way of looking at the problem was not to chase the impossible dream of avoiding security breaches altogether; it was to reduce the business impact of those inevitable events when they did come along.

Based on this insight, Infosys recommended not only getting everything back up and running as quickly as possible, but also implementing a series of measures to build resilience to future attacks.

BREAKTHROUGH

The key was to think not only about recovery but also about resilience to future attacks. Avoiding security breaches altogether is impossible; smart companies also aim to reduce the business impact of those inevitable events when they do come along.

Infosys®

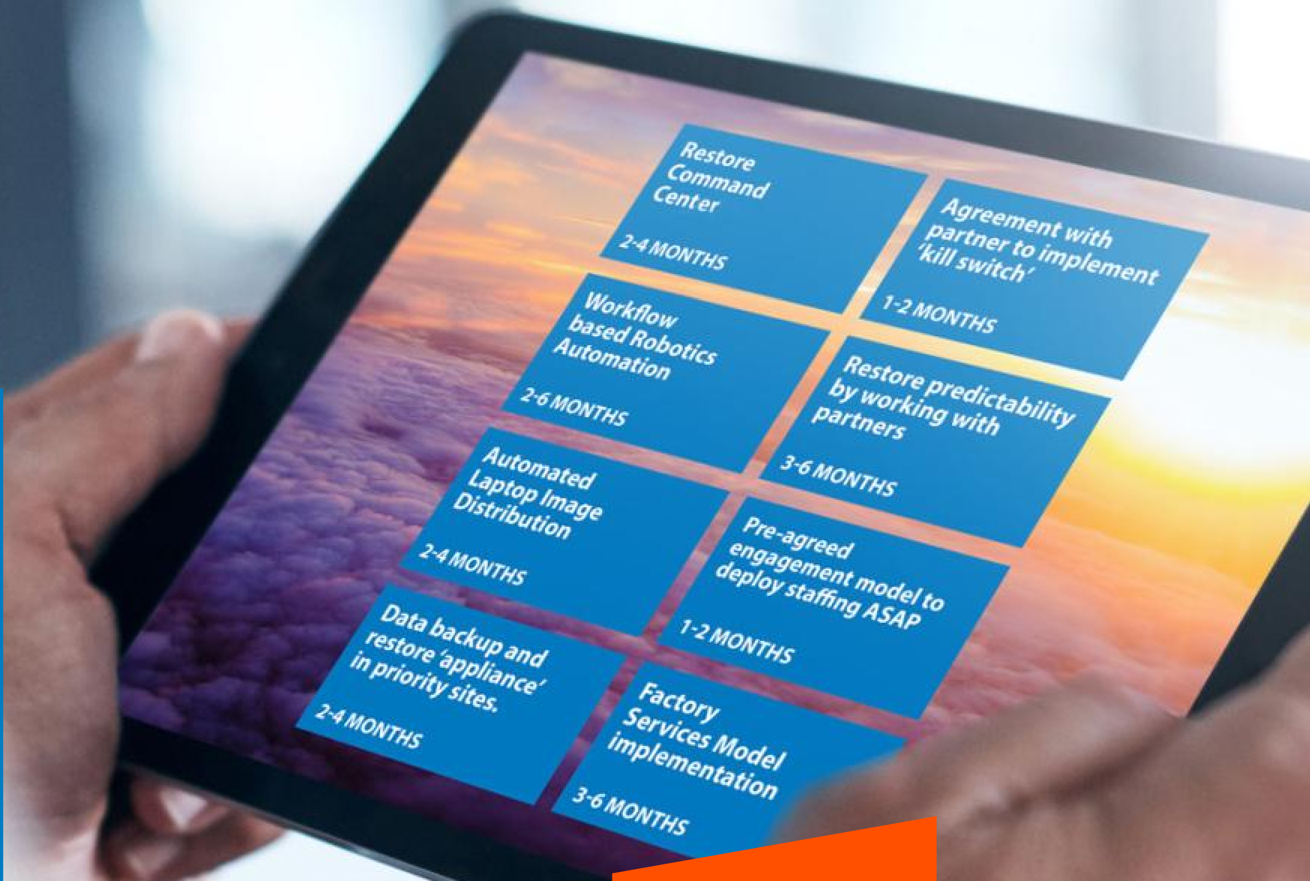
ACTION STATIONS

First up: prevention and detection. Infosys quickly put in place a number of safeguards to reduce the chances of future attacks (whilst practically observing that absolute defense was an impossibility). Enhanced network zoning and firewalls were implemented, web filtering and email security were enhanced, and where possible, vulnerable legacy systems were retired. Meanwhile, a **Cyber Defense Center** was set up featuring a 24x7 Security Operations Center, security monitoring platform, threat intelligence, kill switches, automated incident response procedures, and the ominous sounding Dark Threat detection. The defenses were manned and the systems were ready.

ROAD TO RECOVERY

But more crucially, innovative recovery systems were also put in place. Senior management at the client office knew that most of their competitors would take similar safeguards against attack. The difference would be their ability to respond and become fully operational again. Infosys proposed a number of measures they could take, along with an estimate of how long each would take to implement.

OPTIONS PROPOSED



Restore Command Center
2-4 MONTHS

Agreement with partner to implement 'kill switch'
1-2 MONTHS

Workflow based Robotics Automation
2-6 MONTHS

Restore predictability by working with partners
3-6 MONTHS

Automated Laptop Image Distribution
2-4 MONTHS

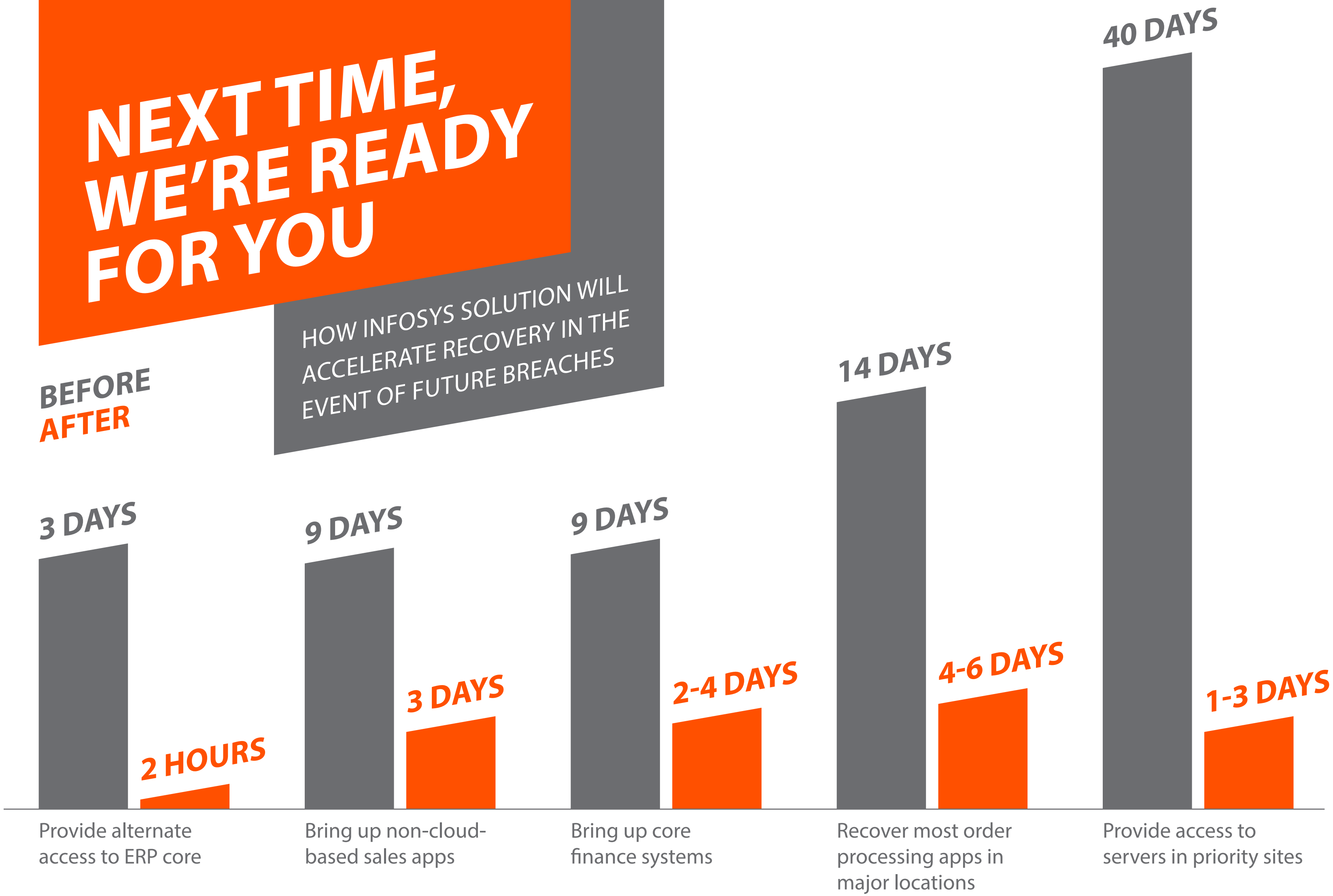
Pre-agreed engagement model to deploy staffing ASAP
1-2 MONTHS

Data backup and restore 'appliance' in priority sites.
2-4 MONTHS

Factory Services Model implementation
3-6 MONTHS

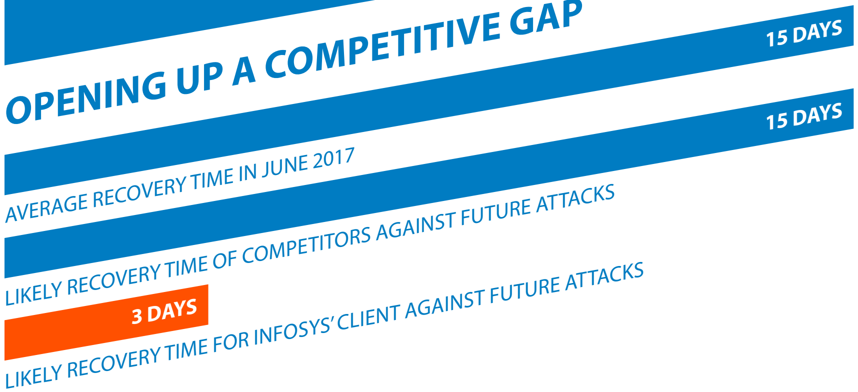
NEXT TIME, WE'RE READY FOR YOU

HOW INFOSYS SOLUTION WILL ACCELERATE RECOVERY IN THE EVENT OF FUTURE BREACHES



Infosys client is ready to be up and running again while the competition is still struggling.

OPENING UP A COMPETITIVE GAP



We can't predict where the next attack will come from – but we know how we will respond.

80%

AVERAGE REDUCTION IN RECOVERY TIME

WE DID THIS FOR THEM. WE CAN DO IT FOR YOU.

Find out more about how we protect our clients against the effects of cyber attack by reaching out to us at askus@infosys.com

Infosys®