proofpoint

DOWNTIME, NOT DISASTER

ENHANCING OFFICE 365 WITH BUSINESS CONTINUITY AND RESILIENCE

INTRODUCTION

Microsoft Office 365 is a big part of a digital transformation that's changing the way we work, collaborate and create. It's a whole new way of doing business. And it comes with a whole new set of risks.

For many IT leaders, the move to Microsoft's cloud-based software platform will prove a career-defining project that will mean the difference between evolving their business or overseeing its stagnation.

Business resilience is critical to a successful migration. Unplanned downtime was a fact of life for IT teams long before the cloud. But as your infrastructure moves to Office 365, outages can be harder to avoid or predict—and have a greater impact.

The typical Office 365 customer experiences three to four outages per year. Some are brief and isolated. But many, like the outage that hit Europe and the Asia-Pacific region in April 2018, can last hours, grinding operations to a halt, straining customer and commercial relationships, and jeopardizing business opportunities.

You can't control when Office 365 goes down or rely on its default security to keep threats from disrupting your operations. But you can build resilience into your organization. IT downtime shouldn't take down your business.

This e-book describes how Office 365 is changing the workplace, the new business continuity challenges that come with it, and what you can do about them.

[1] Ray Schultz (Email Marketing Daily). "Microsoft Email and Office 365 Back After Global Outage." April 2018.

BUSINESS, TRANSFORMED

If your organization is not embracing digital transformation, it won't be around much longer," said Dave Michels, a principal analyst at the research firm TalkingPointz. "There's simply nothing more important for organizational survival than digital transformation."[2]

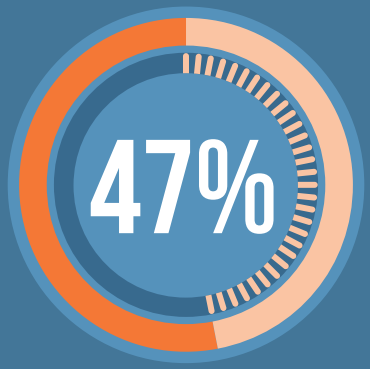
Michels is not alone in his assessment. Digital transformation is already reshaping worker collaboration, business processes, and customer engagement. And in many cases, the impetus is coming from the top.

According to a recent Gartner survey, 47% of CEOs are being pushed by their board of directors to make progress in their digital business. And 56% say their digital efforts have already improved profits.[3] Digital transformation is making workplaces more flexible. It's empowering workers. And it's reducing barriers to teamwork on a global scale.

[2] Dave Michels (Enterprise Connect). "Digitally Transform…or Else." July 2017.

[3] Gartner. "Gartner Survey Shows 42 Percent of CEOs Have Begun Digital Business Transformation." April 2017.

ACCORDING TO GARTNER



of CEOs are being pushed by their board of directors to make progress in their digital business

of CEOs say their digital efforts have already improved profits

> "IN THIS MODEL, NOBODY WILL SEE THEIR MAILBOXES FULL. THEY WILL GET MAIL ON THEIR PHONES, OR BRING THEIR OWN DEVICE, [AND] WE'LL LEVERAGE THE POWER OF THE CLOUD TO STORE MORE, AND USE ONEDRIVE TO COLLABORATE ON DOCUMENTS IN REAL-TIME."
>
> – Zafar Chaudry, Chief Information Officer Cambridge University Hospitals, NHS Foundation

EASIER COLLABORATION

Cambridge University Hospitals' NHS Foundation Trust began migrating to Office 365 in August 2017 to allow its staff to communicate anywhere and more easily collaborate on documents.[4]

Under the NHS's old on-premises email system, workers could email only from their PCs; email piled up in their inboxes and communication was a chore. And when staff needed to work together on a document, someone had to manually collect and reconcile everyone's edits.

"In this model, nobody will see their mailboxes full," Zafar Chaudry, the hospital's chief information officer, told Computerworld UK. "They will get mail on their phones, or bring their own device, [and] we'll leverage the power of the cloud to store more, and use OneDrive to collaborate on documents in real-time."

EMPLOYEE EMPOWERMENT

TD Bank recently adopted Office 365 as part of a broader push to the cloud. Jeff Henderson, the bank's chief information officer, says internal surveys showed that its employees wanted to be able to work on a range of devices, "unchained" from their desks.[5]

"It's much easier for people to work in an agile fashion if we give them mobile capabilities to work that way," Henderson told American Banker, an industry trade newspaper.[6]

[4] Tom Macaulay (Computerworld UK). "How Cambridge University Hospitals plan to use Office 365 to improve patient care." August 2017.

[5] Penny Crosman (American Banker). "TD Bank's tech strategy for becoming a bank of the future." July 2017.

[6] Ibid.

BUSINESS DISRUPTED

No technology is impervious to cyber threats or unplanned outages. As your business moves to the cloud, business resilience is more critical than ever.

That's because business disruption costs money—it can mean lost sales, higher operating costs, fines, contractual penalties, damage to your brand, and more.

Resilience to cyber attacks means quickly detecting and resolving threats—before they cause major business disruption. And resilience to IT outages means keeping users connected and productive no matter how Office 365 is performing.

WHAT IS BUSINESS RESILIENCE?

Business resilience, also called business continuity, is more about weathering disruption than preventing it.

According to SearchCIO, it's "the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity."[7]

The British Standards Institute, the U.K.'s standards-setting body, defines it as "the ability of an organization to anticipate, prepare for, and respond and adapt to incremental change and sudden disruptions in order to survive and prosper."[8]

The concept encompasses everything from risk management to disaster recovery. And in an era of change, especially when it comes to infrastructure you don't own or control, it's more important than ever.

Resilience isn't just about catastrophes, says Gartner research director Peter Firstbrook. It's about but "everyday and continuous threats." [9]

Firstbrook likens resilience to how cities manage emergency services such as police departments, fire stations, and hospitals. City codes and enforcement help reduce crime, prevent fires, and keep people healthy. But trying to avert every crime or emergency would be too expensive and may even hurt citizens' quality of life. That's why cities also need emergency services when something goes wrong.

That's what resilience is about—expecting the unexpected and being ready for it.

[7] Margaret Rouse (SearchCIO). "Essentials Guide: Disaster prevention and mitigation strategies." January 2014.

[8] BSI. "Organizational Resilience: Harnessing experience, embracing opportunity." November 2015.

[9] Heather Pemberton Levy (Gartner). "The Six Principles of Resilience to Manage Digital Security." June 2015.

WHAT HAPPENS WHEN YOUR CLOUD GOES DOWN

IT downtime can cost anywhere from $140,000 to $540,000 per hour, according to Gartner.[10]

Beyond the direct financial costs, IT downtime can compromise your compliance and security. Employees trying to get their work done might use personal email outside of your organization's security and compliance controls.

CYBER ATTACKS ARE COSTLY AND DISRUPTIVE

For cyber attacks, slower responses equal more damage and costlier cleanups. In its annual study of data breach costs, research firm Ponemon Institute found that threats identified 99 days or sooner cost $2.80 million on average. Those that took longer to spot cost $3.83 million.[11]

Lingering cyber threats are also disruptive. A single ransomware attack crippled city services in Atlanta, Georgia, for more than a week in March 2018. Residents couldn't pay their water bills or parking tickets. Court proceedings were cancelled. Police reverted to filing paper reports.[12] The attack cost an estimated $2.7 million to clean up.[13]

Most cyber threats arrive through email. Detecting and resolving them in their earliest stages—ideally, before anyone has a chance to click an unsafe attachment or URL—is the best way to deal with them.

[10] David Gewirtz (ZDNet). "The astonishing hidden and personal costs of IT downtime (and how predictive analytics might help)." May 2017.

[11] Ponemon Institute. "2017 Cost of Data Breach Study Global Overview." June 2017.

[12] Kimberly Hutcherson (CNN). "Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand." March 2018.

[13] Aaron Diamant (WSB-TV). "Ransomware attack cost city $2.7 million, records show." April 2018.

ACCORDING TO GARTNER...

IT downtime can cost anywhere from **$140K to $540K per hour**.[10]

PONEMON INSTITUTE FOUND...

that threats identified 99 days or sooner **cost $2.80 million on average**. Those that took longer to spot **cost $3.83 million**.[11]

WHY ISN'T IT ENOUGH TO SEND UNSAFE EMAIL TO THE JUNK FOLDER?

Attackers know that Office 365 sends unsafe email to the junk folder, still accessible to users. One attack we observed counts on this behavior and gets around it. Here's how it works:

1. The attacker sends malware or an unsafe link to an Office 365 user.
2. Office 365 diverts the email to a junk mail folder.
3. The attacker sends a second, "safe" follow-up email with no malware or malicious link. Office 365 lets it through to the user's main inbox. The email asks the recipient to look for the first email in the junk folder and open it.
4. The user opens the first email, infecting their device or giving up their credentials.

BUILDING A RESILIENT CLOUD

A successful Office 365 deployment requires a plan for business resilience. You need to keep employees connected and productive when Office 365 is down. And you need to keep business running amid a growing deluge of cyber attacks.

FAST, EFFECTIVE RESPONSE TO THREATS

Today's attacks target people, not technology. While Office 365's own infrastructure is well-protected, the people using it may not be. People-centered attacks can be especially difficult to spot because they don't always contain malware or URLs that would normally trigger your defenses.

Most threats arrive in email. A resilient cloud infrastructure blocks most threats before they reach the inbox. But no defense can stop every attack. When something gets through, you also need to be able to detect and contain it quickly.

Whether your email infrastructure is on-premises, in the cloud, or both, your defenses should automatically quarantine and remove threats—not just send them to a junk mail folder.

ACCESS TO EMAIL WHEN OFFICE 365 IS DOWN

You can't prevent Office 365 from going down. But you can prevent outages from disrupting business. An email continuity or failover service lets your users continue sending and receiving email during outages.

Your continuity service should be as simple to use as regular email—or people won't use it. That means users' contacts, calendar, recent emails (sent and received), should be waiting for them. And when Office 365 comes back online, any emails sent or received through the continuity service should already be ready for them in Office 365.

CONCLUSION AND RECOMMENDATIONS

A resiliency plan can mean the difference between downtime and disaster. Here's a three-step strategy to get you started.

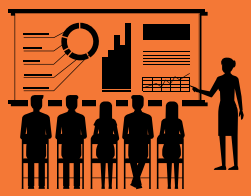
STEP 1: IDENTIFY WHAT'S BUSINESS-CRITICAL AND TIME-SENSITIVE

The first step to building a resiliency plan is pinpointing business-critical and time-sensitive business functions and processes. These include anything that can't be interrupted, even for a short time, without hurting your business. Don't forget to include any resources that support these functions.

For most organizations, email is near the top of that list. And for Office 365 deployments, an outage may also affect files, contacts, calendar appointments and more.

STEP 2: CALCULATE THE COST OF BUSINESS DISRUPTION

The second step is calculating the costs of business disruptions from security incidents and service downtime. Consider every possibility and its relative likelihood. Then determine the costs and benefits of avoiding these outcomes.



STEP 3: CREATE A CONTINUITY PLAN

Expect the unexpected with a continuity plan—before you need it.

Determine what processes and technology you need to keep core business functions running during an Office 365 outage or security incident.

Your plan should include failover processes and procedures so that your organization doesn't miss a beat when something goes wrong. And don't forget to have a plan for smoothly transitioning back normal operations when Office 365 is back up or a threat has been resolved.

Employee training should be a big part of any continuity plan. Teach users how to spot and report email threats. And drill them on what to do in an outage—and things not to do, such as doing business on personal email.

Finally, consider technologies that automate, enhance, and speed up your threat response efforts. The faster you can contain and resolve security incidents, the more resilient your business will be.

PITFALLS TO CONSIDER

Here's a partial list of potential business losses to consider. For a comprehensive list, see the U.S. government's Business Impact Analysis worksheet at Ready.gov.

- Lost sales and income
- Delayed sales or income
- Increased expenses (such as overtime labor, outsourcing, expediting costs, and so on)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans
- Reputational damage
- Cleanup (for security incidents)
- Fines (for compliance incidents)

proofpoint™

LEARN MORE

To learn more about how Proofpoint can make your move to Office 365 successful, visit **proofpoint.com/office365**

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.