BEMO

Microsoft 365
Security & Compliance

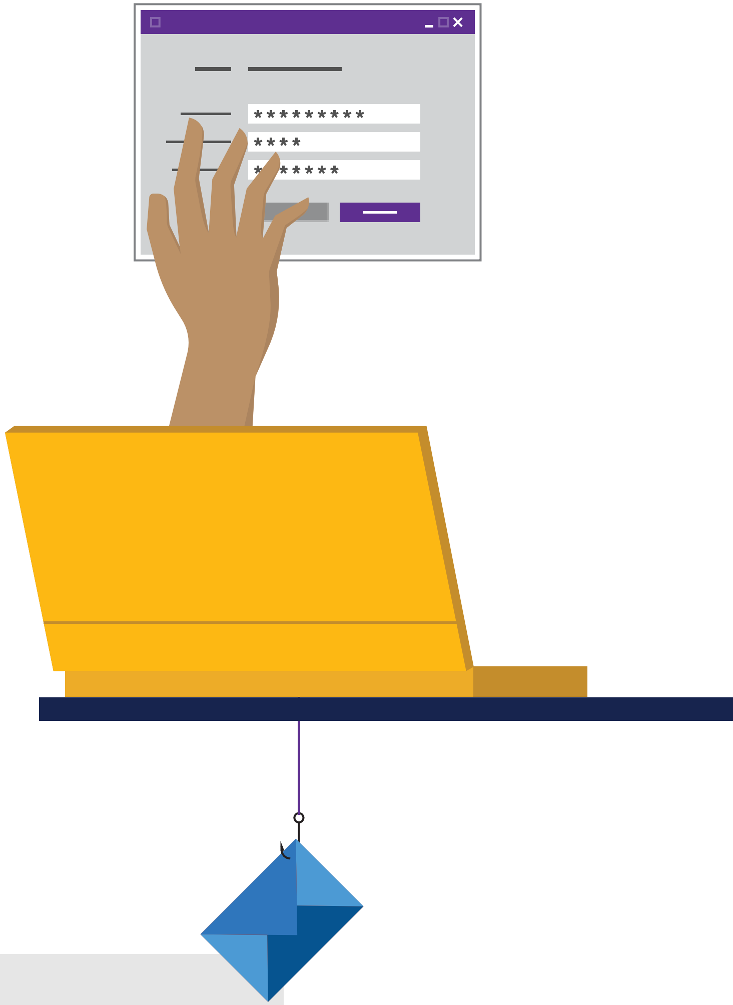
Brandon Lecoq
Cybersecurity Manager

The reality for your business today, and the importance of proactive security

- Cyberthreats pose material risks to your business
- Phishing and ransomware attacks are commonplace and disruptive
- We can help you become secure

Phishing

Broad-based phishing and spear phishing both rely on what’s most often cited as security’s weakest link: people. Phishing can take many shapes, including:



Email links and attachments

Domain spoofs

User impersonation

Domain impersonation

Links to fake SaaS apps

180,000,000–200,000,000

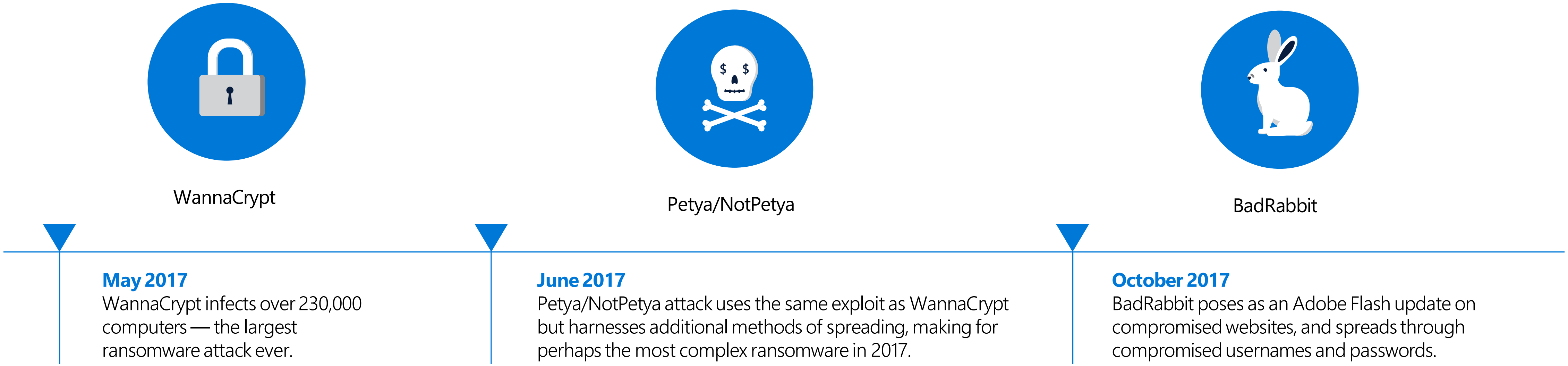
Approximate number of phishing emails Microsoft detected each month, over three months (November 2017 - January 2018).

Ransomware

Ransomware infects and encrypts files (and sometimes entire disks) to prevent access until a ransom is paid—and there's no guarantee victims will regain access.

Ransomware made a real-world impact in 2017, bringing down critical services like hospitals, transportation, and traffic systems. Ransomware families were responsible for the 2017 attacks.

Outbreaks of Various Ransomware Families



WannaCrypt

May 2017
WannaCrypt infects over 230,000 computers — the largest ransomware attack ever.

Petya/NotPetya

June 2017
Petya/NotPetya attack uses the same exploit as WannaCrypt but harnesses additional methods of spreading, making for perhaps the most complex ransomware in 2017.

BadRabbit

October 2017
BadRabbit poses as an Adobe Flash update on compromised websites, and spreads through compromised usernames and passwords.

Introducing Microsoft 365

A complete, intelligent solution that empowers everyone to be creative and work together, securely. Microsoft 365 brings together Office 365, Windows 10, and Enterprise Mobility + Security.

Four core principles of Microsoft 365

- Unlocks creativity
- Built for teamwork
- Integrated for simplicity
- Intelligent security

Microsoft 365 security and compliance scenarios

Microsoft 365 offers a comprehensive set of features to address security and compliance.

Enterprise-Level Identity Protection

Limit access to organizational systems to only the right people

Control and Protect Information

Help ensure docs and emails are viewed only by intended recipients

Proactive Attack Detection and Prevention

Thwart hackers and recover quickly if attacked

Do you have identity protection?

Do you **know** who is accessing your data?

Can you **grant access** to your data based on risk in real time?

Can you quickly **find** and **react** to a breach?

Are users empowered to **work securely** anywhere at any time?

Enterprise-level identity protection

Protect your organization's data from unauthorized access and identity threats.

Safeguard and manage identity:

Manage cloud activities more securely.

Detect and respond to identity-based threats:

Protect identities and proactively prevent compromised identities from being abused.

Protect against password attacks:

Replace passwords with strong two-factor authentication, and better protect credentials against persistent threats.

81%

of all hacking-related breaches use compromised credentials[1]

95%

of phishing attacks that led to a breach were followed by some form of software installation[1]

75%

of individuals use **only** 3 or 4 passwords across all of their accounts[2]

[1] Verizon 2017 Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[2] Security Week Survey (ref. P35 of Security Playbook)

Microsoft 365 Enterprise products

Enterprise-level identity protection

OFFICE 365	WINDOWS 10 ENTERPRISE	ENTERPRISE MOBILITY + SECURITY
Multi-Factor Authentication for Office 365 Advanced Security Management	Windows Hello for Business Windows Credential Guard	Microsoft Azure Active Directory Microsoft Advanced Threat Analytics Cloud App Security

Is your data secure?

Is your data secured **regardless** of where it's stored or shared?

Does a data **compliance policy** control access to sensitive information?

Do you have the ability to **classify** and **encrypt** sensitive data?

How easily can you respond to **eDiscovery** requests?

Control and protect information

Protect your business data while enabling user productivity and collaboration across devices and locations.

Manage cloud application usage:

Get the security of an on-premises system for cloud applications.

Protect against data leakage.

Have control over the access to information, no matter where it's stored or who it's shared with.

Protect against malware and phishing attacks:

Help protect your customers' mailboxes against new malware threats and sophisticated attacks.

Respond to security incidents:

Streamline and speed up document reviews and improve adherence to data retention policies.

88%

of all hacking-related breaches use compromised credentials[1]

$4M

Average cost of data breach for surveyed companies[2]

48%

of survey respondents say their outdated information security controls or architecture are a high area of vulnerability[1]

$158

Cost incurred for each lost or stolen record containing sensitive and confidential information[2]

[1] 2016 EY Global Information Security Survey http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016.

[2] 2016 Ponemon Institute Cost of a Data Breach Study https://securityintelligence.com/media/2016-cost-data-breach-study/

Microsoft 365 Enterprise products

Control and protect information

OFFICE 365	WINDOWS 10 ENTERPRISE	ENTERPRISE MOBILITY + SECURITY
Office 365 Advanced Threat Protection Office 365 Data Loss Prevention Office 365 Customer Lockbox Office 365 Advanced Data Governance Office 365 Advanced eDiscovery	Windows Information Protection	Microsoft Azure Information Protection Cloud App Security Microsoft Intune

Do you have attack detection and prevention?

Do you have tools that allow you to **automatically detect** high-risk usage?

How **quickly** can you react after a breach has been detected?

Can you **automatically guard** users against phishing attacks and dangerous links?

Are you leveraging **machine learning** to uncover suspicious activities?

Proactive attack detection and prevention

Be constantly aware of the current threat landscape to help identify attacks and attackers before they cause damage or disruption.

Risk Assessment:

Take a security assessment to help understand security risks, formulate policies and plan for improvement.

Manage mobile productivity:

Secure access to the cloud helping to protect data on unmanaged devices.

Safeguard messaging:

Zero-day protection to help guard against malware and viruses.

Protect, detect and respond to advanced threats:

Use artificial intelligence, machine learning, and other means to help prevent successful attacks, identify high-risk activity, and quickly respond to contain attacks before damage occurs.

4,000
Ransomware attacks per day in 2016[2]

$1B
Losses from ransomware in 2016[1]

91%
Of cyberattacks start with a phishing email[3]

$1T
Cumulative global spending on cybersecurity products and services over the next five years[4]

[1] https://www.vircom.com/blog/the-10-craziest-cybersecurity-statistics-of-2016/
[2] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
[3] https://phishme.com/2016-enterprise-phishing-susceptibility-report
[4] http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Microsoft 365 Enterprise products

Proactive attack detection and prevention

OFFICE 365	WINDOWS 10 ENTERPRISE	ENTERPRISE MOBILITY + SECURITY
Office 365 Advanced Threat Protection	Windows Defender Advanced Threat Protection	Cloud App Security
Office 365 Threat Intelligence	Windows Defender Security Center	Microsoft Advanced Threat Analytics
Office 365 Security & Compliance Center		

Our Microsoft 365 Security Assessment Offers

BEMO

Pick one, two, or all three of the security assessments below where we will perform detailed analysis of your environments and provide actionable security insights. The ultimate goal: assessing your risks and providing the best solutions to keep your company safe and secure.

Office 365 Security Assessment

- Identifies security objectives
- Uses security analytics tool to render a security configuration score
- Recommendations to balance security and productivity needs
- Provides guidance on successful implementation of Office 365 security features

Shadow IT Assessment

- Provides insights on cloud usage, security objectives, and requirements
- Helps mitigate security threats with Microsoft Cloud App Security
- Creates a Cloud Visibility and Control roadmap

Rapid Cyberattack Assessment Workshop

- Identifies security gaps related to ransomware attacks
- Implements Microsoft 365 readiness specific to ransomware defense
- Creates a remediation plan and a Microsoft 365 roadmap specific to ransomware defense

Our Microsoft 365 Proof of Concept Offer

BEMO

Our 5-day proof of concept offer will help you:

- Understand the security features of Windows 10, Office 365, and Microsoft Enterprise Mobility + Security and how they can be used.
- Prioritize the implementation of the key features and scenarios based on your IT and business context.
- Use hands-on labs with the latest and most advanced security features to protect, detect, and respond to advanced attacks in your IT environment on premises and in the cloud.

Day 1: Fundamental

Consultant will kick off the engagement, conduct key security capability workshop on Microsoft platform, and perform lab preparation

Days 2-4: Hands on Lab Activities

3-4 lab activities from Identity & Access Management, Information Protection, and Threat Protection

Day 5: Gap Analysis Deliverables

- Gap Analysis
- Findings and recommendations
- Closeout
- Questions

Contact us for information and pricing on this comprehensive and exciting offer!

Our Microsoft 365 On-going Security Services Offer

BEMO

Security is an on-going activity. Once you get your IT systems protected and secured, you may need on-going assistance to ensure that systems stay protected and maintained.

We can help! Our ongoing security services can include any or all of the following:

- Implementing and maintaining Microsoft 365 security tools such as Secure Score, Advanced Threat Protection, Attack Simulator, and others
- Patching and updating
- Helping meet and maintain regulatory or other compliance requirements
- Threat response
- Other
- Other

Contact us for information and pricing for on-going security services!

BEMO