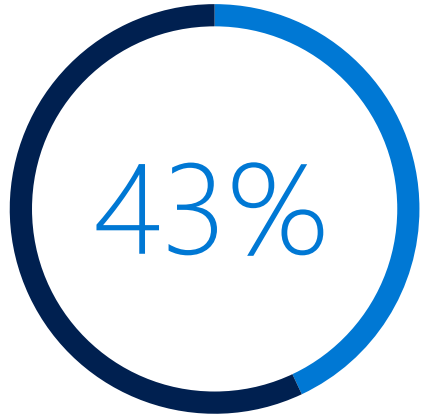


# Protect your organization against cyber threats and information loss

Michael Deacon – Security Architect at NovaQuantum  
17 Sept 2020



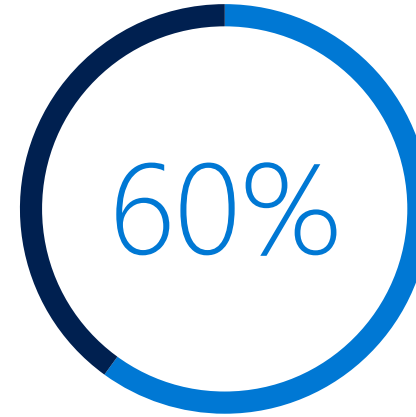
# Threat landscape for small businesses and nonprofits



of cyberattacks target small businesses



Devices are compromised by ransomware every month



of small businesses close their doors after a cyberattack



is the average cyber attack remediation cost for small businesses

# Why are attacks so successful?

It only takes hackers 4 minutes to get in your network, but 99+ days for businesses to discover they've been breached.



# Where are the biggest security pains for nonprofit organizations?

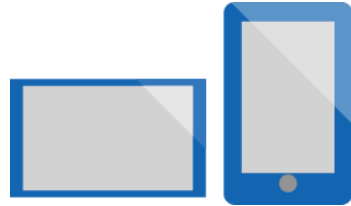


## Email

Subpar antivirus antispam doesn't catch attacks

Users click on ransomware and phishing links

Accidentally send confidential data



## Mobility

One extreme: Prohibit use because of security concerns

Or the other: Don't provide any protection for data on devices



## User credentials

Users have same passwords across all accounts, increasing risk if compromised

Attackers have sophisticated methods to easily steal credentials



## Compliance

Standards don't change based on company size

Requirements for GDPR and other regulations are rigorous and complex

# Why don't nonprofit organizations have the security they need?

Common misconceptions contribute to the problem.



## Security is too complex

While nonprofit and humanitarian organizations may not have in-house IT departments, that doesn't mean they can't implement comprehensive security. Technology and services can radically reduce complexity while also providing strong protection.



## Security is too expensive

SMBs typically spend about **15%** of their budget on security or **\$1,320/user** annually. To increase protection, you don't need to necessarily increase IT spend – just adjust how you are spending your dollars.



## Security is not a mission-critical priority

Nonprofits that deal with confidential donor and beneficiary information – whether they are financial, health care, or humanitarian services – have the same accountability to secure data as big enterprises, so they need enterprise-level protections.

# Microsoft 365 Business

Business savvy way to reduce risk



## Simple

One solution

Cloud platform simplifies deployment



## Reduces costs

Eliminates costs for multiple third-party vendor solutions

Reduces maintenance and management costs



## Secures organization

Security built into your productivity platform

Don't need to make trade-offs to justify security investment

Protect business against risk-related costs

# Microsoft 365 Business security benefits

Safeguard your organization against external threats and leaks



Protect against security threats



Protect business data against leaks



Control who has access to  
business information

# Protect against security threats

Protect inboxes against spam and viruses

Block ransomware and phishing attacks

Keep Windows 10 devices safe from sophisticated malware



<sup>1</sup> Verizon 2017 Breach Investigations Report

<sup>2</sup> Security Week Survey



# Protect your organization against data leaks

Restrict copying and saving of organizational information

Block sharing of sensitive information like credit card numbers

Prevent unauthorized users from opening or viewing sensitive documents

Encrypt data on mobile devices

Wipe data on lost or stolen devices

Back up email in secure archive

<sup>1</sup> 2016 EY Global Information Security Survey <http://www.ey.com/au/en/services/advisory/ey-global-information-security-survey-2016>

<sup>2</sup> <https://www.ibm.com/security/data-breach>



# Control who has access to organizational information

Only let the good guys in

Know who is accessing your data

Keep credentials safe

Confirm identities with multi-factor authentication

Quarantine compromised devices

Prevent non-compliant devices from accessing your systems



<sup>1</sup> [Verizon 2017 Breach Investigations Report](#)

<sup>2</sup> Security Week Survey

Turn to *NovaQuantum* for the expertise you need to help you safeguard your business data. We know IT security and we know Microsoft 365 Business. We can help you control and manage access to sensitive information, protect company data across devices, and guard against unsafe attachments, suspicious links, and other cyber threats.

You can expect guidance, recommendations, and best practices to keep your business data safe from both internal and external threats with a simple, cost-effective solution.

Our audit and remediation services for M365 will:

- Assess your current security state to help us understand how secure your organization really is
- Remediate high priority security concerns and identify security objectives based on strengths, distinctions and uniqueness of your organization
- Deploy Microsoft 365 Business
- Configure advanced security features based on
- Identify and protect sensitive data
- Provide ongoing services based on an actionable security roadmap

[Contact us](#) Today for a Free consultation!

