ITWC The Content Experts

WEBINAR HIGHLIGHT REPORT

# Securing the New Perimeter

BROUGHT TO YOU BY

ITWC

SPONSORED BY

Itergy

Quest

There is no shortage of challenges in the new normal, especially when it comes to supporting and securing employees in the wake of a massive migration to work-from-home (WHM). With inadequate user experience opening the door to workarounds and other security-defeating behaviours, the pressure is on to better equip our remote workforce.

Eager to delve deeper into this issue, ITWC CIO Jim Love joined Ralph Loewen, CEO of Itergy and Curtis Johnstone, Distinguished Engineer/Microsoft MVP at Quest on September 15th for a webinar titled ***People Not Perimeters: How to make work-from-home and cloud architecture more productive and secure***. Hosted by ITWC, the session engaged Love and his guests in a lively discussion of the new WFH reality, with a focus on practical tips for identity management.

Love opened by highlighting the expertise of both Itergy and Quest in managing customer security and resiliency, lauding their collaborative relationship and explaining that using partner tools, like Quest, has made Itergy's Active Directory and Identity proprietary services unique in the world. With over 30 years in business, $1 billion in revenue, and 4,000 employees in 100 countries, Quest has established a reputation for supplying essential software.

## Everyone enjoys a good horror story

The webinar was organized around a series of anecdotes dealing with compromised digital identities. In one example, a consultant for a North American transportation network set off a process that effectively put the brakes on transportation across the country. Another case detailed the plight of a retail customer unable to do credit card transactions for 10 days because their Active Directory crashed. A third story chronicled an outage that lasted the better part of eight hours, and saw almost 10,000 workers in the manufacturing sector sent home from their shifts.

> “If you lose your identity, you can really be out of business until you get it back up and running.
>
> *— Curtis Johnstone, Distinguished Engineer/ Microsoft MVP*

According to Loewen, the important thing for each of these companies is to ask what they could have done differently. Multi-factor authentication (MFA), which according to Microsoft blocks over 99.9 per cent of account compromise attacks, would have made a significant difference. Rigorous monitoring as well would have made a difference by allowing users to detect a breach before it occurred and not after.

## In praise of boring

As a follow-up to the high profile horror stories he shared, Loewen told what he describes as a “really boring story” about a major manufacturer with sites in Canada and around the world. Just before COVID-19 came along, the manufacturer had activated MFA, and as a result was able to thwart malicious attempts to access privileged accounts. “So nothing happened in this story, and it’s actually what we all want,” says Loewen. “Boring is really what we’re after.”

Boring may be the goal, but according to Curtis Johnstone, it’s not always the reality. “At some point, a breach will likely happen,” he said, illustrating his point with some sobering numbers related to business continuity in the face of a breach.

### BUSINESS CONTINUITY IN THE FACE OF A BREACH

- ✓ Mistakes Happen.  Breaches Happen.
- ✓ Have a business continuity plan
- ✓ Have backups and know-how to recover – BEFOREHAND
- ✓ Know your toolset and test the process – BEFOREHAND

**55%** OF DATA BREACHES CAUSED BY INSIDERS

**95M** AD ACCOUNTS UNDER ATTACK DAILY

**14sec** ANOTHER RANSOMWARE ATTACK OCCURS

> “The lesser the identity footprint you have to deal with, the more secure you will be.
>
> *— Curtis Johnstone, Distinguished Engineer/ Microsoft MVP*

One thing Johnstone takes away from Loewen’s horror stories is just how crucial identity is. “If you lose your identity, you can really be out of business until you get it back up and running,” he says.

Another takeaway is the inevitability of downtime, whether it results from “a tiny obscure change, an unintended configuration, an outage of some sort to Active Directory, or ransomware malware.”

## A two-part solution and four key precautions

Fortunately, there’s a two-part solution, for Johnstone, beginning with a business continuity tool kit that contains the processes required and the people to contact in the case of a breach. The second part of the solution, and one he can’t overemphasize, is practicing how to use this toolset before it becomes necessary.

“It’s really important to do whatever you can to prevent that breach in the first place,” he said “But if there is a breach, it’s really important that you plan beforehand to address it.”

From an identity security point of view, Johnstone stressed the importance of monitoring identity systems and using identity protection to prevent breaches, structuring his comments around four key precautions:

1. Making sure identity security basics are covered
2. Cleaning up identities
3. Knowing native identity configuration
4. Practising good governance and monitoring

## A new endpoint

The crux of security issues, according to Johnstone, is that the firewall is no longer the perimeter. “We used to be able to lock down a desktop or a laptop and that did the job,” he recalls. “But now, people want access from home machines, so the user has become the new endpoint.”

With a Statistics Canada survey indicating that 4.6 million Canadians were working from home in July 2020, that's an extensive number of new endpoints to secure. It would be one thing if this aspect of the new normal was merely a passing fancy, but according to McKinsey research, 80 per cent of people questioned reported they enjoyed working from home, and 41 per cent said they were more productive. Further evidence of the post-pandemic endurance of WFH is found in a recent Angus Reid study reporting that only 36 per cent of Canadians working from home (just under one-third of Canada's adult population) will likely go back to their place of work when COVID-19 subsides. WFH, it seems, is here to stay.

## The importance of governance

Governance, in particular, was identified as a critical safeguard of identities in a remote workforce. In a customer story about the explosive growth of the Teams solution during the pandemic, Loewen said that Boards of Governors are now raising governance issues around employees and guests sharing access to highly confidential data during their Teams interactions. IT leaders, he said, are charged with ensuring the right people are accessing the right documents, and containing the vulnerabilities inherent in Teams sprawl.

From a governance perspective, IT leaders are also expected to have a handle on the identity footprint, so that identities don't get lost. "It's really important, especially with privileged identities, to make sure they're locked down," said Loewen. "This goes back to preventing a breach in the first place, which is why we prioritize identity governance."

## Protecting digital identities

Other strategies discussed for protecting identities include:

- Knowing your native options
- Using conditional access policies to lock down WFH resources
- Cleaning up permissions for external guests after virtual team meetings are dissolved
- Having an audit trail
- Maintaining an inventory of licenses

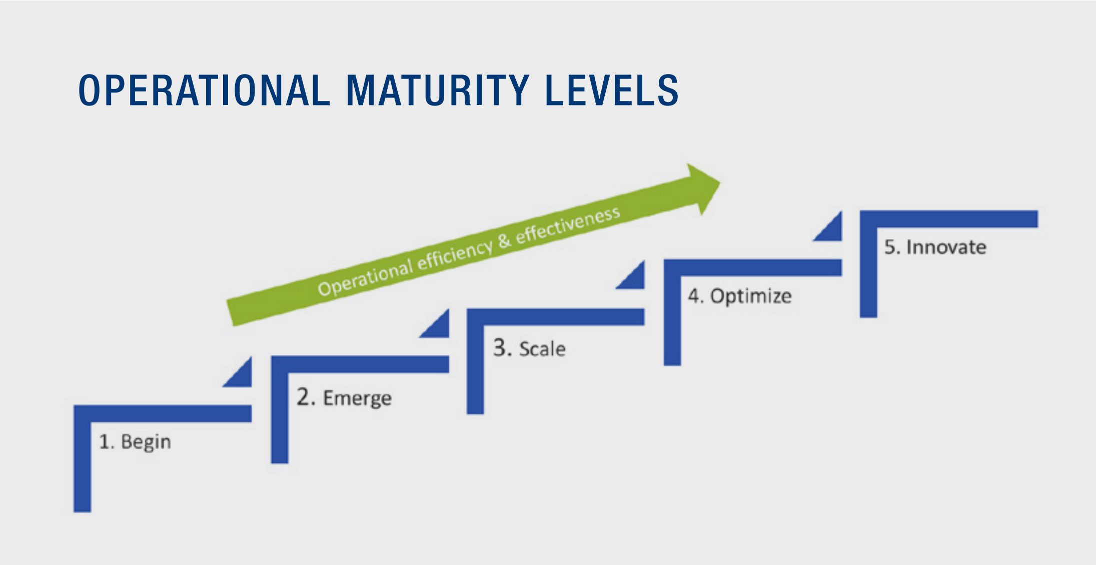
> “We can’t just add people in and forget about them, so we need governance on this. It’s a disaster waiting to happen if we don’t.
>
> *— Ralph Loewen, CEO of Itergy*

Johnstone also advised being especially vigilant during mergers and acquisitions. “That’s when things change and identities get lost,” he says. “Migration is a great time to do a pre-assessment and to clean up any identities – privileged or not – that are not being used. And the lesser the identity footprint you have to deal with, the more secure you will be.”

### How concerned are we?

A poll conducted toward the end of the webinar asked participants to rate their level of concern for the remote workforce. Given that attendees had chosen to attend a webinar related to WFH issues, the results were not surprising. An equal number said they were very concerned (40%) and moderately concerned (40%), with 20% reporting extreme concern.

This sparked a discussion of where organizations need to be in order to relieve this feeling of concern, which in turn led to a consideration of operational maturity levels, and the need to assess recovery point objectives, or how much data the organization can afford to lose.


OPERATIONAL MATURITY LEVELS
Operational efficiency & effectiveness
1. Begin
2. Emerge
3. Scale
4. Optimize
5. Innovate

## A disaster waiting to happen

Even prior to the pandemic, there were problems securing employee identities. One stems from lengthy onboarding processes that involve many layers of permissions and privileges – a challenge when it comes to deactivating an employee's identity. Another obstacle to securing identities is that long-term employees may move jobs multiple times within the same organization, gradually gaining access to highly sensitive, restricted corporate information. When they eventually leave, auditors are faced with finding all the access points and removing permissions.

"We can't just add people in and forget about them, so we need governance on this," said Loewen. "It's a disaster waiting to happen if we don't, but it is a problem that can be managed."

## Taking a page from an Aesop's fable

The recommended approach is along the lines of "slow and steady wins the race," with both Johnstone and Loewen stressing the efficacy of incremental steps.

"We didn't get to where we are overnight, and we won't solve it overnight," said Loewen. "What we need is a strategy in place to move us ahead."

Host Jim Love concurred that small steps are the way to proceed. "We are all facing issues around the massive migration to work-from-home," he said. "We did it really quickly, and now we have to deal with the reality of supporting and securing what amounts to a new enterprise architecture. The best strategy is to know where you are, and keep moving ahead. With every step, no matter how small, you find yourself closer to a good night's sleep."

## About Itergy

Founded in 2001, Itergy provides specialized IT Managed and Project Services that help large and multi-site companies leverage Microsoft technologies to further their operational excellence.  Many of our customers return to us time and again due to our industry-beating SLAs, comprehensive KPIs, clear processes, and problem-solving attitude. We simplify complex IT cloud, hybrid and on-premise environments so our clients can concentrate on their core business. Our areas of specialization include Migration and Consolidation projects, Merger and Acquisition (M&A) projects, Identity and Access, Cloud Infrastructure, Database Platform Management, as well as optimizing Productivity, Collaboration and Business Intelligence.  Simplify your IT.

**www.itergy.com**

## About Quest

With over 30 years in business, $1 billion in revenue, and 4,000 employees in 100 countries, Quest has established a reputation for supplying essential software for solving complex IT challenges.

For over 30 years, we have been turning hype into help for enterprise organizations. Our enterprise software solutions for database and systems management, end-to-end Microsoft solutions, and cybersecurity resilience help organization achieve better productivity and security. Quest provides market leading solutions to deploy next SharePoint or Office 365 migration, replicate Oracle databases, strengthen your cybersecurity resilience for Active Directory, and secure enterprise endpoints. We offer software solutions for what's next. No matter the platform, no matter the challenge — data explosion, cloud expansion, security threats or compliance, Quest has a solution that fits your needs. We're not the company that makes big promises. We're the company that fulfills them.

**www.quest.com**

## About IT World Canada and ITWC

IT World Canada is a media property of ITWC. ITWC is a privately-owned digital media and content services company. Building on over three decades of solid relationships with Canada's technology decision-makers through award-winning excellence in journalism, ITWC delivers incisive, relevant information to executive and managerial audiences. It also provides leading, integrated marketing content strategies to clients, including over 200 global Fortune 1000 companies. ITWC, formerly IT World Canada, is the exclusive Canadian affiliate of International Data Group (IDG) which publishes more than 300 publications worldwide.

**www.itworldcanada.com** **www.itwc.ca**