Upgrading Remote Access Security

Today's Telework Trend

It's no surprise that the far-reaching COVID-19 pandemic accelerated the teleworking trend that started over a decade ago. And while teleworking was already becoming commonplace, at its height, the pandemic pushed up to half of all American workers out of their office or workplace. While some professions will always require face-to-face interaction, the pandemic enlightened executives and management across many industries to the potential cost savings and other benefits that remote work options offer. In addition, the remote model strengthened the viability of collaboration and access technologies.

For employees, teleworking benefits include eliminating the time spent on daily commutes, especially in cities full of congested highways. It has also helped them better manage work and family time conflicts. These benefits are likely related to research that shows teleworking increases job satisfaction and improves retention—which, in turn, saves on hiring and training costs. And while teleworking doesn't always guarantee productivity gains, for many, the potential cost savings and employee attraction is compelling.

The Cost of a Breach

In the Ponemon Institute's fifth annual Cost of a Data Breach report*, they determined that during 2020, the average cost associated with a data breach was $3.86 million. While that cost was flat compared to the previous year, it climbed to $8.2 million in the U.S. Ponemon attributes this rise to increased costs associated with remediation. As usual, the healthcare industry had the highest data breach costs. Worldwide, healthcare breaches averaged $7.1 million, up from $6.45 million the previous year. The second costliest industry, the energy sector, average $6.39 million. As Ponemon points out, industries with higher regulatory bars had higher data breach costs. The more damaging the data breach, the more likely an organization is to lose business, meaning consumer trust—which explains why the healthcare, energy, financial,

2020 Accelerates Remote Workforce Trend

180 organizations participated in the survey.

92% expect an increase in budget for telework technologies.

32% found secure connectivity to be the most challenging aspect of telework.

34% have experienced a breach in 2020 during their telework shift.

Source: LDA Consulting

*www.ponemon.org/

Security Guidelines for Teleworkers

- Review the organization's policies to ensure that teleworker is able to comply
- Secure home Wi-Fi with access security, making sure that the access password is strong
- Protect organizational interaction with a VPN
- Secure all devices to be used for teleworking with strong authentication
- Keep devices current with security updates
- Train teleworkers to recognize suspicious activity and contact help desk

Resource: **nist.gov**

Reasons why corporations are growing their remote workforce:

- Reduced costs in real estate and office space
- Job sharing–people sharing a job, and space
- Flexible schedules, based on needs rather than regimented work times.

Source: from research and work done by Sandy Burud, PhD at **flexpaths.com**

and pharmaceutical industries were some of the hardest hit.

Although Ponemon has conducted this same cost study model for five years in a row, the situation caused by the worldwide COVID-19 pandemic gave the study extra meaning. Seventy percent of respondents predicted that 2020's wave of a remote workforce would significantly increase their cost of a data breach, due to the fact that it would take longer to identify and contain it. With the pandemic changing the remote workforce paradigm, these cost increases merit attention.

Matching Access Security to Risk

Now that remote access for employees, contractors, and other users has risen to a near ubiquitous level, there is a compelling need for a new security model that serves both online and programmatic access—especially since recent events have demonstrated that IT and Security teams can't rely solely on certificates or even private keys for identify verification.

Another important component of securing remote access is usability. Not all resources require the same level of identity verification. Someone accessing the cafeteria menu or general operational information doesn't pose the same level of risk to the organization as someone accessing customer, financial, or other types of sensitive information. Beyond the risk to the organization, process owners might resist higher-access security practices, arguing that they inhibit business operations. And, as we already know, users themselves often respond by finding workarounds or employing social engineering to reduce complexity imposed onto them. In the end, applying access security uniformly to all of the organization's resources doesn't provide meaningful business value.

The following is a generalized list of security practices adapted from various organizations. Let's review some resource access scenarios and explore possible actions that would be appropriate to verify a user's identity:

- **Unclassified business information, general internal information:** Credentials are likely not needed when accessed from known devices used from an expected IP address. Instead of requiring credentials, make it simple and preferably frictionless for your users. If the device isn't known, perhaps allow a simple response such as a claim ID rather than a username/password combination.
- **Resources accessible through single sign-on:** No additional information is needed from the requester after initial user authentication:
  - Corporate organizational information
  - Internal business process resources
  - Unclassified business documents
  - Information disseminated through distribution lists
- Username and password have been the most common means of authentication for over two decades. Whether the user is local or remote, if they are using a known device, there usually isn't a need interrupt them again after the initial authentication because the access to these types of resources is through single sign-on. This same level of classification usually translates into little to no need for VPN protected access. **Personal, sensitive, potentially regulated but unclassified information:** While your organization likely benefits from delivering single sign-on access to these types of resources, there are some variables that need to be evaluated for security. The clearest

exception is regulated information (government, customer, health, HR, etc.). The most common security requirement for these data types is multi-factor authentication for remote access. The other common restriction for remote users is that a VPN or some other encryption technology must be used. Some of these government policies or mandates include a vigorous auditing process whenever there is a data breach—which on its own is a strong incentive to keep access secure. One of the first precautions is to implement a second factor of authentication.

Organizations will likely want to take this same approach for their non-regulated information that is identified as a notable risk to their business. As we have seen in the headlines, retailers and other consumer services suffering from a high-profile breach take a significant financial hit in the short term when it becomes public knowledge, as well as lingering consumer trust issues. In several of these cases, loss of consumer trust damaged revenue for a prolonged period of time and resulted in executives losing their jobs.

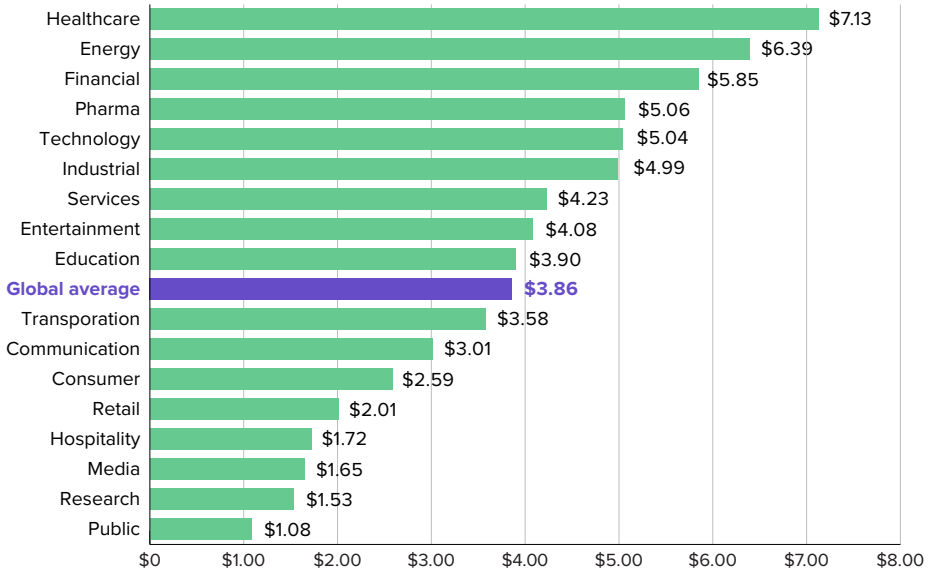
Other internal information that warrants strong authentication includes sensitive financial information and intellectual property. While these types of data don't typically erode consumer confidence, the exposure of internal finances or the loss of IP do exact tangible damage to organization.

- **Confidential or secret:** In the government context, this type of information is labeled as "classified." It qualifies for private access under all circumstances, meaning that multi-factor authentication and VPNs are used all of the time. Although there are notable policy exceptions, secret information qualifies for a zero trust security posture regardless of the context of access. Because mishandling of this type of information can incur criminal penalties, non-repudiation of access is very important.

Some corporations and other non-government organizations might also assign similar protection levels to their private information, driven by the desire to protect trade secrets or comply with laws—such as being sealed for legal proceedings or the timed release of financial information. All of these reasons justify a complete zero trust level of security for this type of information.

Average total cost of data breach by industry

Measured in US$ millions



Source: 2015 Ponemon Breach Study

1 in 4 of organizations in North America have at least some of their employees work remotely

Zero Trust for Remote Access and Beyond

Zero Trust is based on the idea that no access request should be trusted by default. Instead, the identity of the requester be verified first. Although the concept of zero trust originated at the network layer, applying this same approach to the application layer is compelling. It enables organizations to gather and leverage more identity information, as well as enforce a more granular level of access control. While zero trust doesn't differentiate between firewalled environments, it does provide more flexibility to extend beyond the intranet model for cloud-based services. It also provides greater security across the board because zero trust best practices verify requests inside and out.

Least Privilege

As you manage who can do what in your digital world, one common downfall of

7 out of 10
security attacks target small businesses

3 out of 4
breaches are through stolen credentials

breached environments is not staying on top of who has administrative permissions.

Governing Your Users
Satisfying identity governance regulations and managing risk requires organizations to inventory, analyze, and manage their users' access privileges. Beyond having a clear picture of who has permissions to do what, you need to be able to quickly identify and revoke access to resources that users don't need—for example, when users change positions in a company or inadvertently accrues too many privileges. Conversely, a successful implementation must be able to quicky secure approvals from the right information or services owners and automaticity grant them.

Managing Administrator Sprawl
Experts estimate that as many as half of all security breaches come from inside organizations. Insider threats are especially serious when associated with employees who have higher access to systems and information than is needed. Whether access misuse occurs at the hands of an employee or is the work of a cyber criminal who has leveraged the administrator's credentials to gain access to your IT network, you can best manage this risk by closely controlling and monitoring who has administrator privileges and what they are doing with those privileges. The most secure approach is to delegate just enough privilege, rather than distributing root-account credentials to your entire administrative staff.

Recognizing and Reacting to Risk

A core element of secure access is identity verification. In the digital age, that assurance is achieved through some type of a key (typically a username and password) that is almost always required at the beginning of a session. Where warranted, a higher security level is established using various tokens or two-factor authentication—again, at the beginning of the session. These configurations are static and the rules are usually simple, meaning that when a step-up authentication is invoked, it is usually based on simple criteria such as whether the user is remote or the device is known. The defining pattern in these scenarios is that an original level of risk is assessed and adjusted for at the time of the request for access and isn't recalculated for the rest of the session.

With continuous authentication, the system's assessment of whether access to a service should continue can be reassessed. Access metrics are continuously gathered and the risk is continuously recalculated. As IT security groups define the risk models that fit their business, adding predictive capabilities to a zero trust paradigm can drive down user interruptions while increasing security. Unlike traditional authentication approaches, continuous authentication is a closed-loop process. Not only does closed-loop monitoring and control deliver higher security, but the model itself provides more data conducive to behavioral analytics. User behavior analytics can identity out-of-character requests and flag access scenarios as risky where context alone fails. Using unattended machine learning to define the expected digital presence and consumption metrics takes identity-centric metrics far beyond the standard risk data commonly used today.

Two core capabilities are required to make continuous authentication effective:

- **An advanced risk engine** that effectively identifies digital situations where access to data poses a higher or unacceptable risk and where action needs to be taken to gain a stronger confidence level that the claimed identity is accurate.
- **Advanced authentication methods.** The more authentication types that an organization has access to, especially those that are passive, the more flexibility they will have to invoke the right method for the situation at hand. High-risk situations

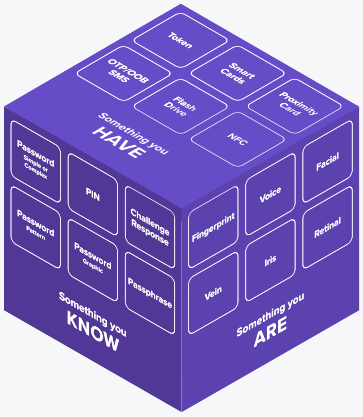
require strong, potentially disruptive authentication methods to verify identity. Passive, low, or frictionless authentication methods will likely provide the needed confidence level to lower risk. Or, perhaps a combination of both types will be needed.

Continuous authorization is the other half of the formula available to protect or mitigate against unacceptable risk. When either contextual or behavioral indicators signal a higher risk situation, the most common response is to invoke a step-up authentication. However, there are also situations or user contexts where a subset of the information is so sensitive that the risk to your organization is at a level where you need to limit access. This is where continuous authorization comes into play. In addition to behavioral or contextual factors that could change the calculated risk during a session, the type of information might also change the risk. You might also need to reduce authorization when the session's authentication strength is low and raise it as it increases. The key shift in security is that access control is no longer a one-time event invoked at the beginning of a user or API session. Rather, it is a continual process that can be re-evaluated at the next access request. Done right, continuous authorization adds a layer of security and usability not previously possible.

Shrinking Authentication to a Small Event

A key step in strengthening the authentication deployment across your organization is to consolidate your authentication silos into a single managed framework. Beyond the hardening effect of having a centrally managed set of authentication policies, it will also optimize the user experience via continuous authentication. Some levels of authentication will need to be invisible whenever possible and be low friction where appropriate. In zero trust security, the default assumption is that every resource request could be from a hostile entity. The more passive authentication options that you have deployed, the easier continuous authentication will be for your users. Consider these options for matching the identity verification strength to the risk posed to your organization. You will most likely find that some of these, or derivatives of them, will meet your security needs and fit your environmental constraints:

Methods of authentication



Micro Focus gives you the freedom to incorporate whatever authentication type that works best for your business.

Contact us at **CyberRes.com**
Like what you read? Share it.

1. **No risk information where the intent is to personalize information:** Passively check browser or device ID markers to identify users. This will also improve the experience by allowing social identities to be federated in conjunction with single sign-on technology
2. **Low risk information:** In addition to identification markers in option one, prompt for a claim ID, which is typically a username or social identity. Other passive options include technologies such as keystroke or voice matching.
3. **Moderate to high-risk access:** A growing set of technological options are available to keep friction low while increasing verification strength.
   - **Passive:** NFC, facial recognition, Bluetooth, voice, typing recognition, smartphone use heuristics
   - **Low friction:** fingerprint, FIDO, challenge, out-of-band authenticators

There are also situations where two or three passive authentication methods can be used together to verify someone's identity with enough confidence to avoid interrupting their activity with an authentication prompt. All of this helps to create a security model that enables your organization to confidently conduct higher risk business operations from anywhere.

Visit the NetIQ Advanced Authentication page to learn more. Watch video demos on our NetIQ Unplugged YouTube channel.

NetIQ is part of CyberRes, a Micro Focus line of business.

CyberRes
A Micro Focus Line of Business