


Technology in the
New Normal:

Maximizing Opportunities, Minimizing Cyber Risks



Introduction

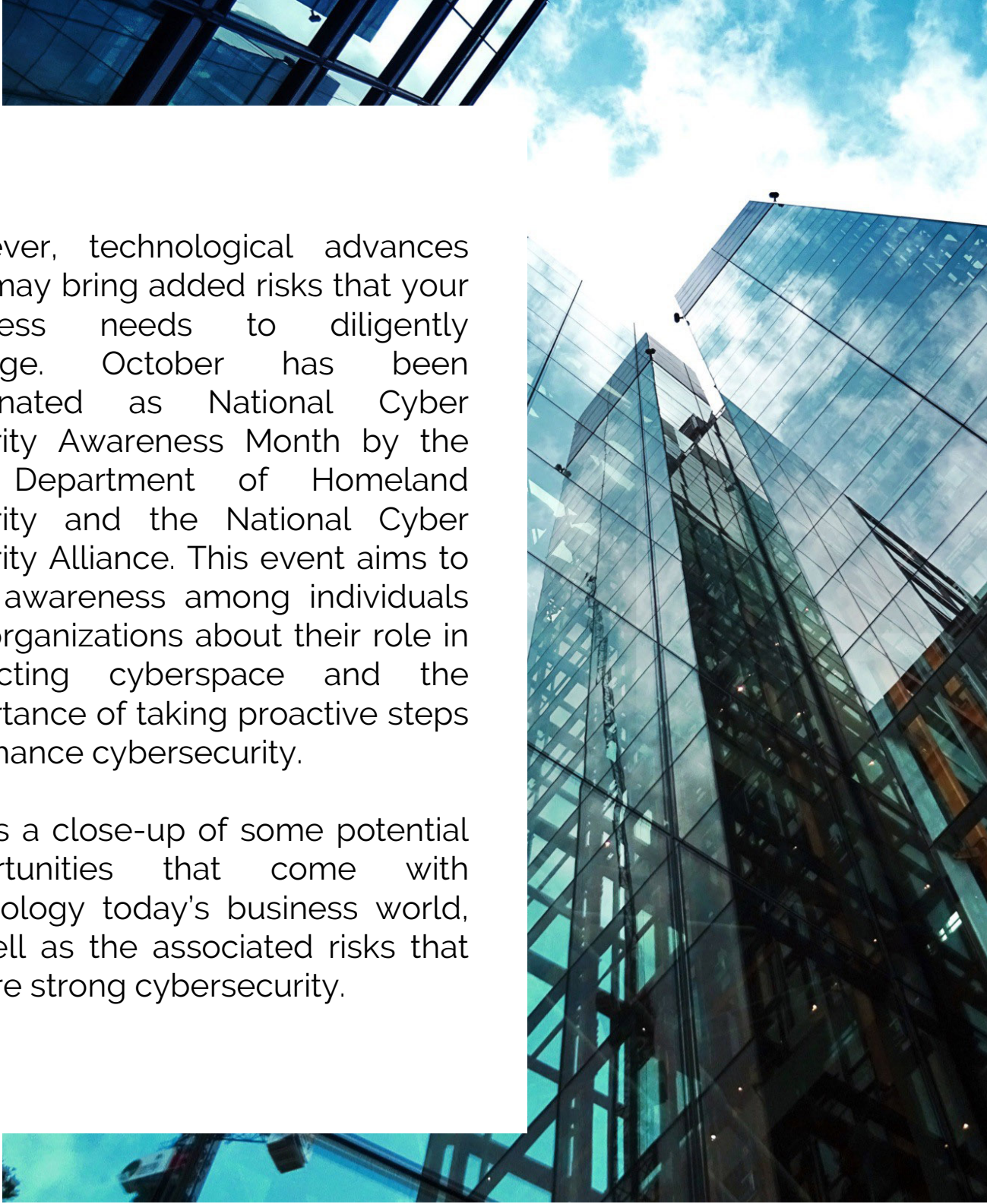


"While we never had to think about some of these issues before the pandemic, it's crucial that we adjust to the 'new normal' and make sure all of our different devices in cyber-land are secure and not susceptible to attack."

Dan Andrea

Partner, Information Security Services

The battle to keep the economy running during the COVID-19 pandemic has proven that technology plays a critical role in our world. Across industries, technology has driven growth for years, but how will its role evolve as we move forward? Technological advances can help your business adjust — and thrive — in today's complex, volatile marketplace.



However, technological advances also may bring added risks that your business needs to diligently manage. October has been designated as National Cyber Security Awareness Month by the U.S. Department of Homeland Security and the National Cyber Security Alliance. This event aims to raise awareness among individuals and organizations about their role in protecting cyberspace and the importance of taking proactive steps to enhance cybersecurity.

Here's a close-up of some potential opportunities that come with technology today's business world, as well as the associated risks that require strong cybersecurity.

Table of Contents

**PAGE 5 SECTION 1 - TECHNOLOGY
OPPORTUNITIES FOR 2020
AND BEYOND**

**PAGE 9 SECTION 2 – NEW
CYBERSECURITY RISKS FOR
2020 AND BEYOND**

Section 1: Technology Opportunities for 2020 and Beyond

Technology Opportunities

Expanded Analytics Can Help Guide Decision Making

Today, organizations collect volumes of data from customers and internal processes that can be used to make more-informed decisions. For example, during the pandemic, governmental and health care officials have turned to analytics for contact tracing. Likewise, tech companies, including Microsoft and Oracle, have built data-based tools to help return employees to the workplace safely.

"Augmented" analytics has emerged as a leading trend for business intelligence platforms. These tools use artificial intelligence (AI) to enhance how businesses explore and process the data. In a nutshell, data preparation and initial analysis, tasks previously performed by humans, can now be fully automated. This allows individuals untrained in IT or analytics to quickly and accurately construct complex models and develop deeper insights. For example, online retailers have applied augmented analytics to formulate multi-channel marketing strategies.

Technology Opportunities

Another area that's gaining ground is graph analytics. This technology goes beyond traditional dashboard reports to identify hidden patterns between entities. Also known as network analytics, it includes techniques for assessing the strength and direction of relationships between businesses, people and more. For example, you might use graph analytics to optimize supply chains or identify social media influencers to help promote your products or services.

Next-Generation AI Focuses on Optimizing Performance

Companies like Google, IBM and Intel are investing millions of dollars into expanding AI technologies, including machine learning (ML) and natural language processing, to help businesses harvest and explore data. For example, operationalized AI can help businesses leverage data collected from customers to deliver the optimal experience. Likewise, ML allows you to test different tactics and strategies and adjust customer interfaces based on the results.

Robotic process automation (RPA), another form of AI, has deployed robots for everything from manufacturing to knowledge work. Basically, any area with repetitive, rules-based tasks that are typically performed manually is a candidate for RPA. It reduces the risk of human error, generally expedites processes and frees up staff for more high-value work.

Intelligent process automation (IPA) takes RPA to another level by incorporating other AI technologies to automate predictions and decision making based on structured and unstructured inputs. IPA is expected to lead to significant improvements in productivity and accuracy, as well as reduced costs.

Both RPA and IPA proved integral to the survival of some businesses when stay-at-home orders were in effect and workers weren't permitted to be physically present in the workplace. Companies that had positive experiences during state-mandated stay-at-home orders are expected to continue ramping up their use of these technologies to protect themselves from future disruptions.

Technology Opportunities

In addition, chatbots are likely to become more popular as ways to enhance the customer experience. Social media have been inundated with complaints about poor customer service since COVID-19 hit the United States hard in March 2020. Some businesses were able to mobilize and have their customer service representatives work from home; however, those businesses generally concede that wait times climbed exponentially and response quality suffered. Improvements in “conversational AI” will empower businesses to handle high call volumes while also personalizing the experience for the caller.

Section 2: With Opportunity Comes Risk – New Cybersecurity Concerns for 2020 and Beyond



Cybersecurity Concerns

Technology-Driven Opportunities Bring Cyber Risks

Technology continues to create opportunities for businesses of all sizes, but it's not without potential pitfalls. For example, U.S. businesses experienced a 17% increase in data breaches in 2019, according to the U.S. Department of Homeland Security. In 2020, the increase in cyberattacks continues, as hackers exploit employees' less-secure home networks to gain access to valuable data and IP assets.

Cybercriminals don't just target large companies. Small businesses with limited resources can be especially vulnerable. In fact, only 23% of small businesses have a formal Internet security program in place, even though 66% of small businesses rely on the Internet, according to the latest data from the National Cyber Security Alliance.

Rather than hacking into an organization's infrastructure, cybercriminals frequently rely on human error. With more employees now working from home during (and likely after) the pandemic — away from much of their companies' on-site safeguards — the risks may be higher than usual.

Cybersecurity Concerns

Phishing schemes have been on the rise as businesses shifted to remote working arrangements. Some scams target individuals with subject lines touting virus vaccines or cures, while others promise information about stimulus payments. Normally, businesses might not be worried about what workers do on their personal devices — but, now, the line between personal and business threats has become blurred.

Increased Number of Endpoints Adds Risk

"The biggest issue right now is the increased amount of endpoints with so many people working remotely. Before the pandemic, in the majority of businesses, only certain people were granted remote access. Now that everyone has access, it opens a can of worms from a control standpoint.

Whether you have children or a spouse working on the same network, the control issues are significant. Not having a clear picture of what is being shared on your network can unknowingly expose you to the bad guys."

-Dan Andrea, Partner, Information Security Services

Employees who click on links in phishing emails sent to their personal email accounts can unleash malware that doesn't discriminate between personal and professional information on their laptops. So, it's critical to ensure your remote workers have — and don't circumvent — the protections they would have in the office.

Cybersecurity Concerns

In late August, the FBI and DHS's Cybersecurity Infrastructure Security Agency issued a joint cybersecurity advisory alert that warned employers about the rise in voice phishing (or vishing) scams targeting remote workers. Here's how these scams typically work:

- The perpetrator (known as a "visher") identifies a target company and researches the social media profiles of its employees. A dossier is compiled for each worker, including his or her name, location, current position, duration at the company and home address.
- The visher sets up a phishing web page that duplicates the company's internal virtual private network (VPN) login page.
- The visher calls an employee on his or her personal cell phone and poses as an internal IT professional with a security concern. He or she gains the employee's trust using information from the social media dossier.
- The visher sends the employee a link to the fake VPN page.
- The unsuspecting employee enters his or her username and password into the domain and clicks the login link, giving the visher free rein to access the company's network.

Vishing scams can be hard to detect because the hacker appears to be a legitimate employee accessing the network remotely through the company's VPN. So, by the time a breach is detected, the company may have already incurred significant losses. Remote workers should be trained on how to detect and report suspicious emails and phone calls.

Cybersecurity Concerns

Potential Risks Extend Beyond Security Breaches

Technological advances may cause another less-malicious problem: data quality issues. To the extent that your company uses operational data to guide decision-making, its analyses are only as reliable as the underlying data. If the data is incomplete, untimely, inaccurate or otherwise invalid, it could lead to misguided decisions.

To avoid this pitfall, your business must establish data quality management (DQM) practices, especially if it's subject to compliance regulations and requirements. Examples include:

- Data monitoring and cleansing,
- Data quality checks, and
- Data lineage management.
- When it comes to DQM, no one-size-fits-all method is available. DQM practices must be tailored to your specific business requirements.

The COVID-19 crisis is expected to have long-lasting effects on the business world. In many cases, the pandemic has served as a catalyst for technological innovations that were already in the pipeline, including shifts to automation, online ordering systems and technology-enabled remote working arrangements.

Businesses that embrace technology can use it to gain competitive advantage. But those that fail to recognize the inherent risks could be sideswiped by cyberattacks or faulty data analytics. We can help you find the right balance between growth-enabling technology investments and cost-effective IT security and DQM practices.

Cybersecurity Concerns

What about Video Conferencing?

When it comes to Zoom, Skype, Teams and WebEx, it's crucial for users to remember to not forward links and to always make sure meetings have a password to enter. When you add a password, it prevents unauthorized users from joining your meetings.

Also, be sure to know your configuration settings; unfortunately, sometimes you can be placed in a situation where individuals start using these meeting applications without thoroughly understanding how to properly configure for security.

Key Takeaway

As we look forward to the rest of 2020 and beyond, it will be crucial for organizations to do several things with regard to allowing remote employee access:

1. Revisit policies and procedures regarding remote access, including its:
 - Remote access policy,
 - Acceptable use policy,
 - Social media policy, and
 - Data classification and use policies.

It's also essential to update the organization's confidentiality agreements as appropriate and to evaluate such issues as whether use of the virtual private network (VPN) is mandatory when working remotely and what types of data employees are allowed to download and store locally.

2. Restrict access to the corporate environment to VPN access with multifactor authentication as part of the user sign in process.
3. Provide continuous security training.
4. Assist users in establishing local firewalls from their remote access point.

We're Here to Help

MEET THE AUTHOR

[Mr. Daniel M. Andrea, CPA, CITP, CISA](#) is a Partner and Director of Information Security Services at KLR. Dan specializes in cybersecurity, social engineering, and data privacy audits and has over 30 years of experience working with clients in a variety of industries.



LET'S TALK

[KLR's Information Security team](#) is asking business owners to inventory their existing cybersecurity practices to identify potential weaknesses in your systems and brainstorm ways to fortify your company's defenses. [Contact us](#) to set up a meeting to discuss potential cybersecurity risks within your business. Cybercriminals are becoming more sophisticated with every passing day and it's no secret that every person, business and network is vulnerable to some form of attack. We can help develop strategies that work for your unique business situation.

ABOUT US

KLR is one of New England's premier accounting and business advisory firms. With 250+ team members and offices in [Boston](#), Newport, Pawtucket, Providence, Shanghai and Waltham, KLR provides a wide range of [services](#) to both individuals and businesses.

Find out why KLR is [so much more than an accounting firm](#) at [KahnLitwin.com](#).

SHARE OUR REPORT

