M+E JOURNAL

Risks & Rewards

The opportunities before media and entertainment are unprecedented. So too are the threats.

OUR CHANGING INDUSTRY
The roadmap to media and entertainment's future is paved with innovation

LOCALIZATION
Content localization is a worldwide, need-it-now business. Here's how to keep pace

WORKFLOWS AND THE CLOUD
Cloud workflows are proving crucial for media productions today

SMART CONTENT
It's a data-driven content reality, and all the tools are there to realize success

21.02

SECURING M&E'S REMOTE WORK REALITY

A host of new cybersecurity concerns — along with both anticipated and unexpected benefits — have emerged

By Chris Tribbey, Editorial Director, MESA

In late 2021 a workplace survey from remote-access tech firm Teradici not only confirmed what the media and entertainment industry already knew, but put an exclamation point behind it: workforces en masse are splitting time between the office and home. And it's a permanent reality.

Ninety-nine percent of more than 8,000 respondents said their workplace will split time between the office and remote settings post-pandemic, and nearly 40 percent said they expect half of their workforce to operate remotely at least twice a week going forward.

But with that convenience comes major security concerns around securing the hybrid workplace in 2022 and beyond, with endpoint security and data integrity both keeping CISOs up at night: ninety-eight percent of respondents said they are concerned about security and data integrity due to employees commuting with endpoint

BECAUSE WE KNOW CHANGE IS A CERTAINTY, we must be ready to adapt the way we will defend. That's why security matters: it's a business of constant evolution, adjusting to the ways we are attacked.

devices, with 90 percent of respondents reporting their companies are using a mix of employee-and corporate-owned devices. Only 10 percent of workers are predominantly using corporate-owned devices, and 74 percent of companies saying they expect more use of employee-owned devices to get their jobs done.

"The pandemic has caused a fundamental shift in how people work, and the 'office' will never be the same," said Ziad Lammam, global head of Teradici Product Management. "As a result of the enormous security concerns associated with unmanaged devices, as well as [bring your own device], organizations are changing how they think about securing their corporate assets. Expect to see companies move away from traditional VPNs to zero trust architectures to shore up their endpoints and protect their data."

Matthew Lane, CEO and co-founder of X Cyber Group, a cybersecurity intelligence and advisory firm, calls this "extension of a company's digital estate" the biggest challenge facing traditional security planning, which historically centered around prioritizing protection of a core network or set of processes, rather than the whole of the system from threats. "That's now been rendered almost entirely redundant," he said.

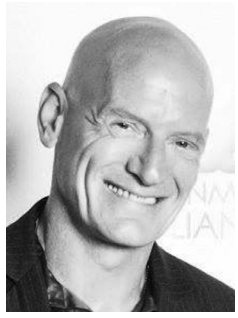
"Companies are having to both trust their employees, but at the same time recognize that previously novel risks are now a key potential threat: people's home networks and personal devices are in essence an extension of the corporate," Lane said. "Digital sprawl, where well-meaning employees set up workarounds and temporary solutions — especially virtual storage — become part of a firm's footprint, likely outside of the cybersecurity team's knowledge, and therefore protection."

A mid-2021 report "Remote Workflow Optimization Game Plan," jointly released by video workflow platform firm Shift and geolocation security specialist GeoComply, touched on this salient point around the adoption of services and platforms for remote workspaces: even if your home network is safe, workers are back on the go post-vaccine, and will take their devices to airports, coffee shops, hotels and more. To combat the threats presented by vulnerable public networks, your remote employees better be setting up virtual private networks (VPNs), look into geolocation-based security and location fraud detection, and work with cloud providers with file transfer security and watermarking features.

"Remote workflows open a huge opportunity for cyber theft and digital attacks, with an enormous amount of sensitive content in transit every day," the report read. "Recorded meetings, confidential legal documents, and pre-release video content are especially vulnerable. Features like watermarks and viewer reporting will deter those who are considering bad choices and make it easier to track down those who do."

Kurt Mueffelmann, global COO and U.S. president of archTIS, which provides software solutions for secure collaboration of sensitive information, pointed to research showing that nearly 80 percent of companies see data leakage as the greatest potential threat to remote work. Yet many are still relying on user training and reactive behavior monitoring and perimeter-based technologies to protect them from the threat vector of trusted employees with legitimate access to applications and systems.

"While these technologies serve an important purpose, they don't proactively address data loss from simple human error and malicious users with legitimate access to



***Chris Tribbey** is the editorial director for MESA. An award-winning journalist, he's previously covered the media and entertainment industry for Variety, The Hollywood Reporter, Home Media Magazine and Broadcasting & Cable.*
chris.tribbey@mesaonline.org
@CCTribbey

data," Mueffelmann said. "To effectively protect against these risks a new approach is needed. A data-centric policy-based approach based on zero trust is a far more effective methodology to ensure data remains secure.

"To protect [intellectual property] organizations need to assess what data an employee needs to access do their job. But it doesn't stop there," he added. "They also need to determine what a user should be able to do with that content if they are granted access to it. Just because you can access a file doesn't mean you should have carte blanche with it."

And, during the pandemic, there's been a noticeable security cost associated with the shift to remote working, according to the 2021 edition of IBM Security's annual "Cost of a Data Breach Report." It found a $1 million-plus cost difference where remote work was a factor in causing a breach, vs. those where remote work wasn't a factor. Up until mid-2021, the percentage of companies where remote work was a factor in a breach was at 17.5 percent, and organizations that had more than 50 percent of their workforce working remotely took nearly 60 days longer to identify and contain breaches, compared to companies with 50 percent or less working remotely, according to the report.

"Higher data breach costs are yet another added expense for businesses in the wake of rapid technology shifts during the pandemic," said Chris McCurdy, worldwide VP and GM of IBM Security. "While data breach costs reached a record high over the past year, the report also showed positive signs about the impact of modern security tactics, such as AI, automation and the adoption of a zero-trust approach — which may pay off in reducing the cost of these incidents further down the line."

For Ted Harrington, co-owner and executive partner of cybersecurity consulting firm Independent Security Evaluators (ISE), there's no doubt work-from-home has fundamentally changed how enterprises protect information. In the pre-pandemic world, the enterprise could control its own network environment, but as we've collectively moved to work from home, "now you're having people working on their own networks, with personal equipment, and these systems and networks are not as well-secured as the enterprise. And the enterprise now has to think about how it's going to deal with that," he said.

Of course, issuing equipment to remote workers is one way to address security issues, but it's the adoption of secure cloud systems that may be more important, Harrington said. "Enterprises are able to provide access to information by leveraging a more secure cloud service rather than relying on someone working locally from their home environment, and that's a pretty significant upgrade from a security and operational perspective," he added.

And there's a little-discussed benefits that's come about with this shift to mass remote working, Harrington noted: "The awareness of these issues is a lot higher now. Companies are talking about cybersecurity now, not just within the security and tech teams, not just within leadership, but across the entire organization, the entire rank and file. That's a very positive thing, because as people start talking about security issues, it starts to drive behavioral change in a meaningful way," he said.

"We can't predict what's going to change, but what we can predict is that things will change. Because we know change is a certainty, we must be ready to adapt the way we will defend. That's why security matters: it's a business of constant evolution, adjusting to the ways we are attacked." ⊞