The Video Migraine

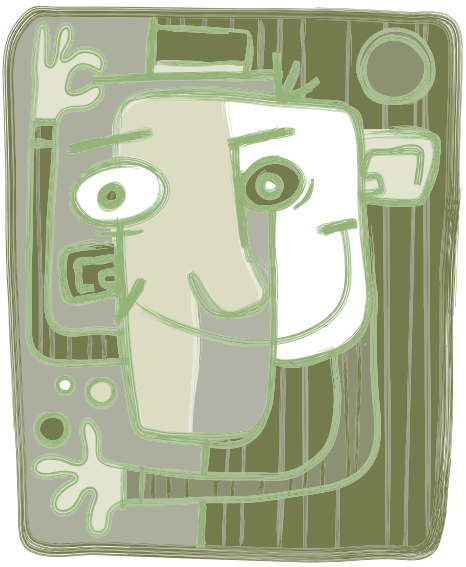
SECURITY, GOVERNANCE, AND BUSINESS CONTINUITY—ONE STEP AT A TIME

BY **DOUG HOWARD**

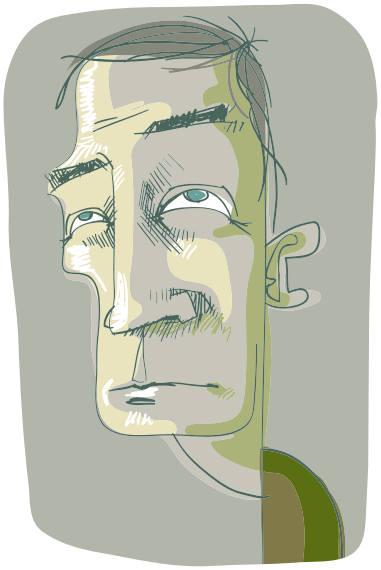
Migraines are caused by many triggers, and for some people (in reality, many) video has been a clear root cause. If you're on the hook for a high-profile video conference or streaming event, your nervous system is preconditioned for a heightened sense of awareness and stress the day of the event. Your nervous system is likely to go through four stages of change on the route to a migraine: prodrome, aura, attack and postdrome. Here's how it plays out:

PRODROME The early symptom is the stress that pulsates through your body as you mentally review all the things you and your team did to prepare for anything you could have missed or that might go wrong. So many things outside of your control. So many points of failure. Will the network holdup? Did the firewall get changed? Did anything change since you did the test an hour ago?

AURA The inability to focus comes quickly as things don't work as expected. The call dropped … how hard is it to just reconnect? Why am I the only one that knows how to do this? The remote users can't join the stream and continue to hit the connection over, and over, and over, and over again, exacerbating the problem. Is the room spinning? Why is this taking so long? Why is everyone looking at me?



ATTACK The pain is in full effect now. How could this have happened? How could we have missed that? Everything was working before. They say it's not the network. How long will the pain last. You're the last stop for the blame train. Your head is pounding and you can't think straight. What will happen now?



POSTDROME OK, breathe, let's figure out what happened and make sure it doesn't happen ever again … assuming I still have a job. How will I recover from this? Man I have a headache. Where are the aspirin and how soon can I get a drink or three? I think I've aged 50 years.

Even if everything goes perfectly, your body assumes the worst and forces your nervous system into believing the worst will occur just as it has so many times before. The net result … the VIDEO MIGRAINE.

Introducing or expanding video across an enterprise provides significant business value … but not without risk. Video within an enterprise, like any application, introduces new considerations that have wide-reaching impacts on the business and IT alike. The positive benefits to a business that use video are boundless, but video can also be very dangerous if not properly planned and managed. Video, unlike most applications, introduces both requirements and impacts associated with latency and bandwidth to an extreme degree, as well as security and Business Continuity and Disaster Recovery (BCDR) demands. Also, because video is part of your Unified Communications and Collaboration (UCC) suite, it often falls under one or more compliance and regulatory requirements. In all cases it falls under U.S. state and international privacy and Personal Identifiable Information (PII) laws. Video is also a broad term that encompasses Video Teleconferencing Conferencing (VTC), Streaming Video, and Video on Demand (VOD). Endless business applications fall under video as well, including desktop, room and telepresence for VTC, webcasting, executive and financial/product broadcast, IPTV, process monitoring and surveillance for live and hybrid streaming, on-demand training, enterprise YouTube, compliance archiving, and publishing fall under VOD.

Video should be considered a key element to support your overall corporate BCDR plan, providing a rich communications conduit during critical times. This doesn't count all the other supporting categories such as lecture capture, editing, content management/storage, and video intelligence. One last complication is video delivery, which includes variables such as frequency of use, inside/outside the firewall routing and transversal, transmuxing/transcoding, automatic network condition detection and adjusting, and integration with other business applications that may reside on premise or In the Cloud (ITC).

As with all things revolving around IT, it's often overwhelming to know where and when to start. We recommend starting before the next purchase or add-on order. After all, if your network, the Internet, conference rooms and studios, audio systems, viewer platforms and standards were static and you never introduced new and add-on devices and applications, you'd never get a video migraine!

VENDOR AUDIT AND MANAGEMENT WITHIN THE IT SECURITY DISCIPLINE

Many companies are required by law or their own business needs to perform vendor oversight, ensuring the vendor has adequate information security and data protection incorporated into its products and services. In truth, every organization must secure its environments in the face of changing technologies, people and

processes. Before adding an IT vendor's product or service to your organization's operational profile, you must first set your own standards for IT security, governance and business continuity. You may choose from a few primary routes for such a policy:

1) Adopt the international series of standards, presently the ISO 27000 series

2) Adopt the free written policies used by your country's government, such as the US NIST standards

3) Adopt a uniquely created standard. ISO/IEC 27001 formally specifies a management system to bring information security under explicit management control. A formal specification means that it mandates specific requirements so organizations can be formally audited and certified compliant. While ISO has expenses for purchasing the standards, it's globally recognized and provides a well-developed base outline for an organization to build unique standards around.

The ISO 2700 series are primarily designed around securing and enterprise, but with a little creativity they can be used for auditing and evaluating your vendors. The ISO standard contains 12 main sections that can be mapped specifically to the evaluation of any vendor. They include:

1. **Risk Assessment**—What is the general risk of doing business with the vendor (i.e. financial viability, technical solution, deployment options and requirements, etc.)
2. **Security policy**—What is the vendor's written security policy
3. **Organization of information security**—Governance of information security
4. **Asset management**—Inventory, classification and prioritization of information assets and services
5. **Human resources security**—Security aspects for employees joining, moving within and leaving an organization
6. **Physical and environmental security**—Protection of the physical users' computers and devices and the datacenter facilities
7. **Communications and operations management**—Management of technical security controls in systems and networks
8. **Access control**—Restriction of access rights to networks, systems, applications, functions and data
9. **Information systems acquisition, development and maintenance**—Building security into applications
10. **Information security incident management**—Anticipating and responding appropriately to information security breaches
11. **Business continuity management**—Protecting, maintaining and recovering business-critical processes and systems
12. **Compliance**—Ensuring conformance with information security policies, standards, laws and regulations

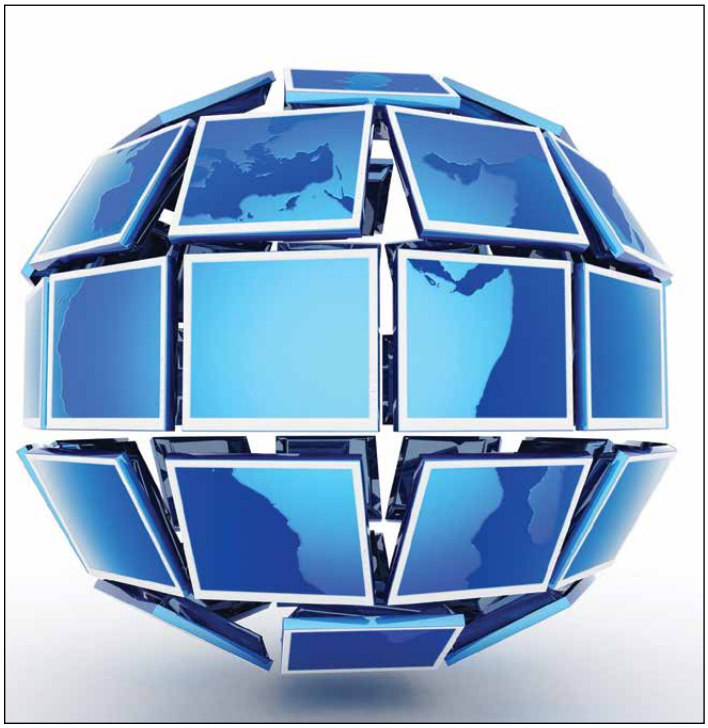
Now the real complication is making sure that all your standards meet the following criteria:

1) actually make you more secure

2) can be supported by your organization and properly managed to the standards you document

3) fulfill your governance requirements so you can provide proper reporting on all the regulatory and compliance standards your organization is subject to

4) continue to be applicable even when the inevitable adversity strikes and your infrastructure, people, and processes continue to operate at a minimal level to sustain the business needs.



In order to properly evaluate a vendor, we recommend a simple three-staged process in auditing and managing the vendor relationship ongoing. Ultimately, you can use this snapshot to demonstrate regulatory compliance, contractual compliance and adherence to best practices for information security practices:

1. **Collect information**—Issue a detailed questionnaire to your vendors. This should be a contractual commitment in your Master Service Agreement, and the replies should be contractually binding.
2. **Verify**—Conduct telephone and on-site visits to verify the responses to the questionnaire and to identify other gap areas not mentioned by the vendors.
3. **Analyze and Report**—Draft and deliver a final report that identifies areas of strengths and weaknesses as measured against your organization's defined standards. We suggest allowing your vendor to review and provide comments to the report.
4. **Determine Acceptance**—You must now judge if the introduction of the vendor into your operations lets you to maintain your acceptable risk level for the business.
5. **Manager**—Assuming you're comfortable with the vendor, your report provides a point-in-time analysis of the vendor and a risk profile. It should also fulfill the following:

a. Provide a list of remediation items and agreed-upon vendor actions and timeframe to correct the most critical open-risk items.

b. Have a defined schedule for auditing and reevaluating the vendor (typically every 12-18 months or when a major change occurs.)

These were just a small sample of key points you must take into consideration when evaluating a vendor and the vendor's introduction into your environment does not increase your risk profile. This is the magic of properly creating, testing, and updating a security, governance, and business continuity Program. A well-defined vendor audit and management program supports your business and ensures that the information security controls are operating effectively to protect customer and employee personal information and company trade secrets while creating a measurable assessment of how your outsourcing vendors protect your data.

CONCLUSION

So, as you digest all the things that could go wrong, take a pause. The "aha moment" will hit you and you'll know why so many VTC calls and streamed events fail to deliver positive results most of the time.

Each of these topics could justify a full-length book. Rather, we've committed to writing several "to the point" articles over the next year. In the next article, "Removing the Video Gremlins: Knowing What's Wrong Before the Big Event," we'll discuss best practices to ensure your video infrastructure is ready for use. We plan on outlining a clear case that—when properly planned and tested regularly—video can be provided consistently, at a high quality … without a migraine. **TPO**

ABOUT THE AUTHOR

Doug Howard consults with the **Human Productivity Lab** specializing in helping organizations to ensure video solutions, and other business applications, meet the customers' business value expectation and are deployed in a manner that properly fit into their governance, security, and BCDR programs. Howard is the founder and CEO of Savanture, where he draws upon his experience in governance, security and BCDR from his prior roles including vice president of Security and Business Continuity at AT&T, COO of BT Counterpane, the security division of BT, chief strategy officer of SilverCloud (previously Perimeter e-Security), and his video and UCC expertise from his role as president of USA.NET and prior position as CEO of VBrick Systems.

Howard resides just outside of Washington, DC and can be reached at Doug@HumanProductivityLab.com.