Automate Processes to Manage IT Risk

Collect and analyze data more quickly

By Daniel T. Yunker and John Norenberg

The solutions for mitigating and managing information technology (IT) and cyber risk have always resided in the information collected by the hardware and software. The challenge has been performing anything more than rudimentary analyses on such a voluminous amount of data against increasingly complicated threats and problems. New and improved methods will not only collect the information but also quickly analyze it. The new tools will help transform how IT risk is managed and ultimately mitigated.

Historically, IT risk management has been the province of the IT and internal audit departments. Over the past decade or two, a third group that started as part of IT but is now often separate has emerged—the cybersecurity team. However, the emergence of this third group has not always changed how IT risk is managed. Typically, the different teams own their own domains, work collegially with each other when needed, sometimes prioritize their work based on the latest high-profile problems, and report to the board on a regular basis.

Current state of risk management

The result of managing risk with three separate groups has several less-than-positive results.

Reactive rather than proactive responses

Out of necessity the risk management is almost entirely reactive—closing the barn doors after the horses are all out, so to speak. No in-the-moment management of the risk occurs, only a lukewarm effort after the fact to ensure that the problem does not happen again.

Inefficient tools

The tools to determine that in-the-moment risk management is measured and mitigated—for example, statistically relevant sample testing of processes by internal audit and monitoring of historical data by IT—simply do not do the job. Most audits take weeks—or even months—to complete with data that are exactly that old when reported on, or IT takes weeks to react to something that happens in milliseconds. Again, the horses are out of the barn.

Siloed tools

Both the IT and cybersecurity teams use an enormous number of tools that often are not integrated. On one hand, some of these tools allow for a more real-time analysis of the information in the individual tool. On the other hand, the challenge with this environment is that most of the difficult problems require information analysis across multiple platforms.

In a nonintegrated state, this analysis might take much more time and generate numerous errors due to the manual nature. While this manual effort takes place closer to real time than the previous two points, the costs to perform the work are growing at a rate that is often unsustainable.

Complacent leadership

Many of the most pernicious IT risks are just accepted as a cost of doing business. For instance, one does not need to be a chief information office in a healthcare provider organization for very long before appreciating the value of every single second that an electronic medical record (EMR) system is down or performing poorly.

When you have system problems, the heads of all the emergency departments line up to share with you their calculation of the cost. And yet, that cost of downtime, which for today's purposes includes any time a system

IT risks should not just be accepted as a cost of doing business.

Most difficult problems require information analysis across multiple platforms.

is not performing to specification, is rarely tracked or reported on, much less actively managed.

Computer technology to manage IT risk

Consider the rapid expansion in the reach of computer technology in the past two decades. Almost everything meaningful is controlled by a computer. The enterprise computer has become a part of the regular, direct patient care experience. For instance, the enterprise electronic medical record (EMR) system directly controls intravenous pumps used to infuse medications. Think about it: Patients have a needle in them that potentially is subject to a computer error.

Yet the methods often used to mitigate IT risk remain mostly disintegrated, manually intensive and insufficient to deal with some of the more dangerous risks.

Historically, three factors need to be in place before a new computing system can transform processes:

- The data required for the transformation need to be available or gathered in the appropriate volume.
- The computer system needs to be sufficiently powerful to run the application software that works on the data.
- The transforming application, which typically is made up of dozens or hundreds of sub-applications, needs to be tightly integrated.

Computer systems, just by running, generate a ton of data, which is referred to as logging, and the data files are logs. Every component of a computer, including the software that is running, generates a log entry for everything the system does. In fact, every EMR system, by regulation, must log everything that every user does to guard against medical record fraud.

As you can imagine, the information to sleuth out any IT problem is already somewhere in the logs. Unfortunately, complete analysis is generally impossible for one person to do for any problem. The obstacles include the sheer amount of data, the separate logs generated by all the components, and the need to merge and manage the data from multiple logs to find all the evidence to solve a problem.

Powerful computers are required to process large amounts of data—and remember that the computers processing the data create more data on their own. Furthermore, because every piece of hardware and software creates its own data logs, to be ultimately usable, the data must be merged based on several different key attributes such as user, process and location.

In IT parlance, “the math is not hard, there’s just a lot of it.” As a result, access to significant processing power is required. The good news is that computer processing and cost have, as usually happens, caught up to the problem, and hardware now exists to do the processing.

As indicated earlier, the log analysis tools have largely been standalone tools, specific to the hardware or software that generated them. Other tools have promised to integrate the logs, but they require significant custom programming efforts to develop and maintain for the simplest of analyses.

Consequently, log analysis generally has been confined to the truly curious with time on their hands, a rarity in most IT shops. However, this past year or so, new tools have emerged in the marketplace. The tools use log data and direct-connect integrations into hardware and software, and they provide the IT and cybersecurity staffs with an integrated look at the status of the systems.

Benefits of automation to manage IT risk

Sometime soon, IT cybersecurity and IT audit management will have the tools available to automate the work and transform data into a more valuable asset, as IT has done in other areas of business. The following examples show the benefits of this automation and transformation and are merely three instances of the multitude of areas where value might be found.

Analysis

Picture archiving and communication systems (PACSs) used by healthcare systems often are chronically unstable, no matter the vendor, and crash on an intermittent basis. An analyst at one provider organization worked hundreds of hours researching the logs and found that, within that data, the system was providing ample warning that a crash was coming in the next six to seven days.

The team was able to replace intermittent four-hour downtimes with scheduled 25-minute outages and ultimately eliminate them completely. If the team had access to the right automation, that work could have been completed in a handful of hours rather than hundreds of hours. The analyst might have been able to put his skills to other valuable use.

Auditing

Every EMR system logs every action that every user takes in real time. With this information, internal audit teams can completely transform the practice of access assurance. Instead of managers having to undertake an annual review of each user or run a time-consuming statistically based test, the right automation tools can compare users' actual activity against their job description, credentials and activity history. Any anomalies can be discovered immediately and investigated and mitigated in near real time.

Threat hunting

One of the jobs that cybersecurity analysts perform is called threat hunting. In this role, the analyst tracks down potential threats or illicit incursions into the environment, determines how activities were accomplished, and then shuts them down and eliminates that path from future use. At this point, because the easy incursions have been shut down for years, cybercriminals use very complicated techniques that cross multiple system components.

The good news is that no matter how hard cybercriminals work to cover their tracks, they do leave evidence behind. The problem lies in the fact that these tracks are in a multitude of systems that the analyst traditionally had to traverse manually. Where this data has been integrated with automation tools, the time to hunt individual threats has dropped from days, weeks and months to hours, days and weeks.

Final step: Changing how work is done

Once the right data, sufficient processing power and integrated systems are in place, one last step in an IT-supported transformation will occur. The step will change how those involved in the transformation can work to take advantage of the information at hand and the insights that computer systems can offer.

As in most transformations, the end state of the new methods of working are unclear at the start of the transformation and a period of trial and error is necessary. Even in the best of times, this transformation process can become unnerving when a supposedly well-designed process does not yield the expected results. At worst, the process transformation can be totally abandoned.

So, while the end state might be uncertain, a few outcomes are likely.

Facts replace intuition – Computers ultimately will use facts to reach decisions that currently might be based on intuition.

Relationships change – The new data-rich environment will illuminate the negative consequences of work silos. Breaking down the silos likely will necessitate the creation of new team structures and the relationships needed to maximize the teams' effectiveness.

Harder problems emerge – When the old, easy problems are moved to the computer to manage, the much harder problems emerge and become apparent. Solving these problems might have a dramatic effect on the organization's risk position.

Looking ahead

Organizations that complete this uncomfortable process redesign can reap rewards in productivity, risk mitigation and ultimately efficiency. Once the data and processing power are in place and the integration is emerging, begin considering how to take advantage of the integration to the benefit of your organization.

Starting can be as easy as asking some simple yet provocative questions.

More efficient audits – Do any reasons exist why full data set audits in real time cannot be performed? If not, which of your audits are good candidates to use in pilots?

More effective cyber assessments – Are you satisfied with the operational effectiveness of your cyber assessments? Are you reacting to threats as soon as they become live in

Analysis, auditing and threat hunting can benefit from automation.

Downtime can be defined as any time a system performs poorly against its specifications.

your environment? Can you raise your confidence that you are properly defending against cybercriminals?

Reduced system downtime – If you define downtime as any time any system performs poorly against its specifications, are you happy with the results? Do you even measure them? If you are pleased with your results, how hard are you working to get to an improved state, and is a better way possible?

Final thoughts

Getting to the desired end state is important but can also be difficult. In healthcare, clinicians and the patients that healthcare organizations serve depend on successful IT risk management, accurate internal audits, and stable, safe IT systems. They deserve the very best that can be delivered. Now is the time to get to work. **NP**

Dan Yunker is a principal in the healthcare risk consulting group at Crowe. He has an extensive background in leading healthcare organizations. Dan can be reached at Dan.Yunker@crowe.com and 312-899-1514.

John Norenberg is a senior manager in the healthcare risk consulting group at Crowe. He has previous experience as a senior healthcare IT executive leader in clinical operations, revenue cycle, population health, and IT strategy and infrastructure. John can be reached at John.Norenberg@crowe.com and 630-574-1634.

© Glasbergen/ glasbergen.com

"My keyboard doesn't work, my shredder is jammed, my monitor has gone dark and I'm missing a wheel from my chair. Does my cubicle qualify for disability benefits?"