Multifunctional Copy Machines Have Benefits, Risks

by Tim McClorey, Risk Manager, and Patrick Cummings, Information Services Manager

IT SEEMS THAT each passing day brings astonishing new advancements in information technology. From more powerful copiers and desktop computers to smaller, faster notebooks, tablets and mobile phones, we demand more and more from the technology we use at home and at work. As we strive to improve workplace productivity, we need our tech tools to run as efficiently as possible.

Of course, such advancements come with increased risk of data breach, identity theft, and other exposures relating to information and the technology that helps us store, share, and apply it.

Not just a copy machine
Think about the last time you shopped for a copy machine. It’s a safe bet that your main considerations were pages per minute, fax and email capability, color printing, scanning, sorting, stapling, and other multifunctional uses to improve productivity.

Copier manufacturers have made these and other options possible by adapting technologies from other corners of the industry. The result? These days, copiers do much more than simply copy.

Today, nearly all copiers contain computer hard drives that store thousands of bits of information, which can include everything they’ve copied, scanned, or printed. As stewards of sensitive information, we have an obligation to ensure that the data stored on our copiers’ hard drives is safeguarded appropriately.

Sensitive data is everywhere
To some degree, the level of concern depends on the type of information you manage. Some organizations must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other federal regulations regarding the safety and security of personal information.

Beyond medical records, your office might also copy, scan, or print these types of data:
> Checks and other payroll information
> Income tax information
> Bank account statements
> Employee and/or constituent identification information

Potential exposures
It can be daunting to consider how much private, sensitive information could be stored on your copier hard drive. It’s even more disconcerting to think about what might happen if that information got into the wrong hands. It could be a gold mine for those who are constantly on the lookout to take advantage of today’s technology and its inherent risks.

Misuse of data is especially likely if you have no idea what will happen to your old copier when you replace it. Most outdated machines end up on the resale market, and data could easily fall into the wrong hands.

Fortunately, there are many ways to protect your office and safeguard the sensitive information handled in your workplace. See sidebar on page 4 for ways to reduce exposure to losses from an unintentional data breach.

continued on page 4
Risk Avoidance Program Gets Significant Enhancements

by Cara Kowal, Manager of Risk Management Services

One example is Northwestern University’s School of Police Staff and Command (SPSC). The SPSC is an intensive, ten-week program, conducted one week per month, that prepares law enforcement managers for senior positions.

The cost for one officer to attend approaches $4,000, which doesn’t include the cost of lodging, meals, and overtime for backfilling the officer’s duties while they attend. With municipal budgets becoming leaner than ever, it’s increasingly difficult for departments to afford to send staff to such valuable training.

**CAPs have benefits, costs**

Departmental accreditations, such as the Commission on Accreditation for Law Enforcement Agencies (CALEA) and the American Public Works Association (APWA) Certification, are also very costly.

Department size, community population, and available services are all factored into the costs associated with CAPs. Due to the required paperwork, policy review, and inspection processes, these certifications can sometimes take years.

The MMRMA Board voted to provide $250,000 in RAP funding specifically dedicated to CAPs. Their action affirms the Board’s commitment to help members become recognized leaders in their fields. MMRMA’s risk control staff has identified CAPs that qualify for RAP grants and recommended funding levels to the Membership Committee. This committee reviews an average of 75 RAP applications at each quarterly meeting.

**RAP grants do not reimburse** for lodging, mileage, and overtime costs. Grants for departmental certifications such as CALEA and APWA are capped at $15,000 per year.

**More information online**

Members can find a complete list of approved programs, application forms, and recent grants at www.mmrma.org. RAP grant applications are due 30 days before the Membership Committee’s next quarterly meeting.

**Check mmrma.org** for a list of approved programs, application forms, and recently approved RAP grants.

---

**Risk Avoidance Program Gets Significant Enhancements**

One example is Northwestern University’s School of Police Staff and Command (SPSC). The SPSC is an intensive, ten-week program, conducted one week per month, that prepares law enforcement managers for senior positions.

The cost for one officer to attend approaches $4,000, which doesn’t include the cost of lodging, meals, and overtime for backfilling the officer’s duties while they attend. With municipal budgets becoming leaner than ever, it’s increasingly difficult for departments to afford to send staff to such valuable training.

**CAPs have benefits, costs**

Departmental accreditations, such as the Commission on Accreditation for Law Enforcement Agencies (CALEA) and the American Public Works Association (APWA) Certification, are also very costly.

Department size, community population, and available services are all factored into the costs associated with CAPs. Due to the required paperwork, policy review, and inspection processes, these certifications can sometimes take years.

The MMRMA Board voted to provide $250,000 in RAP funding specifically dedicated to CAPs. Their action affirms the Board’s commitment to help members become recognized leaders in their fields. MMRMA’s risk control staff has identified CAPs that qualify for RAP grants and recommended funding levels to the Membership Committee. This committee reviews an average of 75 RAP applications at each quarterly meeting.

**Initial programs approved**

At its November meeting, the committee approved an initial list of eligible CAPs based on staff recommendations. MMRMA anticipates that this list will expand as members submit applications for a variety of other CAPs.

In addition to approving specific accreditation programs, the Membership Committee also voted to fund CAPs at a rate of 75% reimbursement for associated tuition and implementation fees.

**More information online**

Members can find a complete list of approved programs, application forms, and recent grants at www.mmrma.org. RAP grant applications are due 30 days before the Membership Committee’s next quarterly meeting.

For more information on RAP grants and deadlines, contact Cara Kowal, Manager of Risk Management Services, at 734-513-0300 or ckowal@mmrma.org.

---

**The next deadline for applications is January 30, 2015.**
Excellent 2014 Performance Results in Reserve Reduction

by Michael Rhyner
Executive Director

EACH OCTOBER, MMRMA’s Board of Directors receives, reviews, and accepts a host of financial reports for the prior fiscal year. These reports are summarized in my most recent Quarterly Report to Members, which registered users can read on our website.

At its October meeting, the Board accepted the Audited Financial Statements for the fiscal year ending June 30, 2014. The Board also received and accepted the report from our consulting actuary about changes in needed reserves for unpaid losses and related contingencies.

Reserves trend downward
At the end of a fiscal period, a consulting actuary prepares reserves, which serve as an estimate of the funds to be held by an insurance company or pool to meet its obligation for current and prior year unpaid claims and related expenses. This includes both reported and IBNR (incurred but not reported) losses.

For Fiscal Year 2014, the actuary’s report indicated a further reduction in reserves. Using actuarial methods, all prior year claims, including paid and unpaid open claims, are analyzed and the ultimate dollar value is estimated for each prior year by type of coverage. The actuary also includes a contingency for prior year losses that have yet to be reported or submitted to MMRMA. The result of the analysis is a recommended reserve amount that is then recorded on our financial statement.

The good news is that, for the past four years, the actuary has recommended that our reserves be reduced due to better than expected results. This means that the estimate of the ultimate value of all prior year losses is lower than the actuary’s estimate that was calculated a year ago. This is called favorable loss development.

Accordingly, reducing our reserves increases MMRMA’s net assets, which makes more funds available for distribution to current renewing members next year.

Converging influences
Several factors contribute to the favorable trend, starting with member responsiveness to risk control. Our reserve reductions have been led by some of our most challenging types of coverage: law enforcement and public officials liability.

Data indicate that the use of Tasers in law enforcement has resulted in fewer and less severe excessive use of force claims. Our focus on losses related to employment and land use claims has also been beneficial, and we have also seen a reduction in automobile liability claims.

A cautionary note
Of course, we cannot expect our reserves to trend lower indefinitely. While risk control programs are extremely important, we are always susceptible to unpredictable and random events, due to the size and complexity of the functions we cover.

We must remain mindful, as ever, of potential new and emerging exposures that we may not have anticipated. Unexpected changes in immunities and the judicial environment could also have negative effects.

Therefore, it is important that our reserves are evaluated annually and adjusted accordingly, with the understanding that events and situations will likely result in a strengthening of reserves at some point in the future.

For the last four years, however, lower claims costs have been a highly favorable trend—an accomplishment that reflects our members’ commitment to ongoing risk management practices.
Risks of Copier Data Theft, continued from page 1

Managing risk
Standard risk management practice is to identify the exposure, outline an action plan, take corrective action, and monitor those actions to ensure their effectiveness.

To assist in this process, we recommend developing a policy or procedure to ensure that when a copier is replaced, all previous steps are followed. This will greatly reduce the chance that you will ever see a claim arising from theft of data stored on a copier’s hard drive.

Removing and destroying a copier’s hard drive is the best way to safeguard data.

MMRMA has always been a leader in proactive risk management practices and in providing coverage when things go wrong.

If a claim arises out of information stored on copiers you’ve traded in or sold, MMRMA has your back. In July 2013, we introduced Data Breach and Privacy Liability Coverage, which addresses claims of this type.

There is no doubt that tech advancements will keep on coming. We can also be certain that solid risk management practices and coverage are the best tools for reducing related exposures, no matter where technology takes us.

Reduce The Risk of Copier Data Theft

Use the erase function. Newer copy machines have a “scrub” feature that erases copied, printed, and/or scanned images from the hard drive. Most also have an automatic erase function you can set to “on.”

Take advantage of built-in security features. Your copier may have advanced features for network security, file encryption, and password-protected documents.

Run the erase utility on copiers you take out of service. Make sure you run the erase utility before disconnecting and removing a copier from your facility.

If you can, remove the hard drive before trading in an older copier. Un-delete utilities on copiers allow someone to extract deleted files from the hard drives. For this reason, the safest action is to take out the copier’s hard drive before you trade it in. Most vendors will give you the hard drive without charge if you lease or purchase your next copier from them.

Archive scanned files appropriately. If you use your copy machine to scan files to a “scanned” folder on your network, make sure these files are archived and/or deleted in accordance with your organization’s document retention policy.