****

**Hey STUPID! IT’S NOT A MIMEOGRAPH,
It’s a computer!**

June 2022

*By Gordon Graham*

Editor’s note: This article is part of a series. [*Click here*](https://www.lexipol.com/resources/blog/a-little-knowledge-does-not-make-an-expert/) for the previous article.

Gordon Graham here with some continuing thoughts on Family Eight of the [10 Families of Risk](https://www.lexipol.com/resources/blog/are-you-biased-when-it-comes-to-risk-management/)—technology risks. In my [last article](https://www.lexipol.com/resources/blog/a-little-knowledge-does-not-make-an-expert/), I closed with the following:

Between now and our next visit, find out how much your department paid for the copy machine in your Internal Affairs or Intelligence unit. Seriously—this will be a big part of my next article.

So here we are with the next article. About a decade ago I was doing a program on law enforcement intelligence unit risks, covering the issues involved with gathering intelligence, vetting it for accuracy, storing it securely, [sharing it with other agencies](https://www.lexipol.com/resources/webinars/one-mission-intelligence-sharing-in-corrections-and-law-enforcement/), using it appropriately, redacting it properly prior to distribution, and safely retaining and destroying it.

The location for this program was inside a law enforcement building in a conference room inside the intelligence unit. The separation between this room and the rest of the unit operations was a glass wall, allowing vision into and out of the room. My audience was a mixed group of intel operators from the region.

Throughout the program I saw a lot of people coming into the intel unit and using the copy machine, making copies and leaving with these copies. As I mentioned several times in my last writing, I am a tech idiot, but I do know a bit, and it was obvious to me that this was a communal copy machine—it was used by other people from other units in the organization.

To me this sharing of a copy machine was not a good idea. In my little world, any department needs to have some basic security concerning access to the area where intel operators work. It was also apparent there were no access restrictions to the copier itself—no access code or user identity required. Further, I noticed some of users were young adults—clearly not sworn personnel.

While I have never worked in an intel unit, I have visited a lot of law enforcement agencies over the last 40 years, and my general experience has been that the intel unit is oftentimes located in a separate facility and that security is extremely tight—in many cases requiring escort of people not assigned to the unit and certainly not sharing electronics (e.g., computers, radios, copiers, scanners) with other people in the organization.

Not to digress, but I heard a great story (and you have to wonder if this could possibly be true) from an FBI Special Agent (are there any regular agents?) about a fellow who was scheduled for his interview for an IT job inside the Bureau. He was a good-looking young man and he showed up early for his interview, signed in and started a conversation with the receptionist, which led to him asking, “I forgot to print out my resume—can you do that for me?” The person behind the counter agreed and he provided a “stick” which was then inserted into the desk computer and he gave instructions on how to access the resume and it was then printed and he took his “stick” back.

Sometime later he was summoned by the person doing the interview for this IT job he was seeking. During the interview he was asked, “Do you actually think you could [hack into our system](https://www.police1.com/officer-safety/articles/ransomware-gangs-get-more-aggressive-against-le-IYRBBMy7JZkLp1YH/)?” His response: “I did that this morning while I was waiting for you.” Then he displayed his PC and what he had learned from the information he stole from the receptionist’s computer via the “stick.”

But back to my focus (as if I am capable of focusing) of this writing. In the agency where I was doing my work on intel risks, I could see my observations were mirrored by other people (remember, it was a mixed group from other departments) and during a break in the program, I heard others expressing concern about “security” in this facility.

Further on in the program I identified some attendees who worked in the agency hosting the program and I asked some questions—and I was very disappointed. Basic security was nonexistent. I heard statements like, “I know him, he is a good kid—he is a summer intern” and “They use our copier when theirs is down” and other silliness.

I could ramble on and on but I then asked the question, “How much did you pay for this copy machine?” No one knew, so I asked one of the host agency cops to find out—and trust me I could stretch this into five articles—but the bottom line was that it was not purchased but instead leased; that the involved copshop did not do the lease but rather the lease was done by County Purchasing; and that this particular copy machine was relatively new because the lease on the preceding copy machine was up. When I asked what happened to the last copier, I was told it was taken away by the people who brought in the new machine.

By then “the bells of St. Mary” were clanging in my head. It became very apparent this copy machine was being treated like a “mimeograph” (if you do not know how to drive a clutch you will have to Google that) rather than a “computer.” The personnel in this intel unit had failed to understand that every document “copied” was stored in a hard drive inside the machine—and that when the old copier was taken away, so was a copy of all the documents ever copied by that machine.

I am approaching my word limit so I will go back to the focus in my last writing. [Who is your chief technology officer](https://www.lexipol.com/resources/blog/a-little-knowledge-does-not-make-an-expert/) (CTO)? Is your CTO really a CTO or just smarter than anyone else in the room? I could write another five articles on this topic, including malware, software purchases, use of [unsecured WiFi systems](https://www.lexipol.com/resources/blog/dont-loan-your-wi-fi-to-sex-offenders/), hardware purchases (one of my favorite recollections is the agency that bought five years of computers in advance, not recognizing that by the time that first computer was delivered, it was already out of date from a tech capability standpoint—and there are five more years of this model coming to the agency), password security, and another dozen issues.

In our next piece I will give you a few hints on how to hire a CTO for your agency and close out with some horror stories with the hope they will scare you into recognizing all the risks involved in Family Eight.

**Timely Takeaway—**Who hired your current CTO and what do they really know?

Gordon Graham is a 33-year veteran of law enforcement and is the co-founder of [Lexipol](http://info.lexipol.com/nysacop), where he serves on the current board of directors. A practicing attorney, Graham focuses on managing risk in public safety operations and has presented a commonsense approach to risk management to hundreds of thousands of public safety professionals around the world. He holds a master’s degree in Safety and Systems Management from University of Southern California and a Juris Doctorate from Western State University.