Mid-Term in IS342:
Questions from Upper Management

The IS342 Management of Information Assurance course< http://www.mekabay.com/courses/academic/norwich/is342/index.htm > is halfway through this semester's work. At mid-term, I provide a mid-term multiple-choice exam and also give students a couple of weeks to respond to memos supposedly from high-level executives to them as if they were Chief Information Security Officers (CISOs) in industry. Their essays are graded simply on a 10–9-8–0 scale:

- *10: This is great! Could even be published!*
- *9: Good work. Solid, concise, no significant errors.*
- *8: At the limit of professional acceptability – has a few grammatical or spelling errors or some minor imprecision*
- *0: Unacceptable: factual errors, rudeness, disruptive bad writing….*

I was so pleased by the responses written by student Gregory Antonellis to the current mid-term memo-exam that I have obtained his permission to publish his memos.

* * *

1. FROM: Edward J. Olmos, Director of IT Operations
TO: YOU as CISO
RE: Using MacroHard Wurd on multiple systems

Hello. I'm sorry to tell you that your recent actions have caused quite a ruckus in the IT department. I know that you were recently an ISSO in government service, but you have to understand that things are different here at the Lurwatzer Corporation. We bought the master copy of MH Wurd at Staples perfectly legally. We own that software now, so we installed it on all 827 workstations running MH FrenchDoors v11, as we are entitled to do. The Wurd package cost us over $430, so I think you will understand that we've paid our fees for the product and can use it freely inside our corporation as long as we don't allow our employees to bring copies home to their personal computers. We do obey all laws and principles of ethical behavior here. So in conclusion, I think you're going to have to back off this ridiculous proposal for us to pay $3,000 for a "site license" that supposedly covers up to 1,000 installations in an organization. We can use the money for better purposes than that.

FROM: Gregory Antonellis CISO
TO: Edward J. Olmos, Director of IT Operations
SUBJECT: re: Using MacroHard Wurd on multiple systems

Mr Olmos,

I'd like to state that I'm sorry if my actions have disrupted the IT dept. I believe you are very mistaken about our use of MH Wurd on company workstations. We do not own that software. We own a license to use a copy of it. To use the software in a way that violates said license gives the publisher grounds to file a lawsuit against Lurwatzer Corporation in civil court and may also be a violation of civil law. I assure you, installing a retail copy of MH Wurd on over 800 workstations is definitely in violation of the license agreement with which that product was sold, seeing as MacroHard does not sell volume or site licenses in retail form. The various licenses available in retail stores allow installation on between one and ten workstations. Whether or not these workstations are internal, external, privately owned or on Mars makes no difference a violation of the license is still a violation of the license, which is grossly unethical. I stand by my statement that we purchase a site license. I am of the belief that safeguarding the

company from a lawsuit and the effects that lawsuit would have on our reputation is a perfectly good purpose for which to allocate $3000. If this is not possible then we should reconsider our use of MH Wurd and consider more affordable alternatives. If you feel I have made these statements in error, please contact me so we can arrange a time to meet in person.

Sincerey,
Gregory Antonellis, CISO

* * *

2. FROM: Mary McDonnell, CIO
TO: YOU as CISO
RE: Software development project

Thanks for your excellent presentation yesterday on your proposals for how to start our first internal software development project. This is pretty exciting, because it's only recently that we have seen a cost/benefit ratio that justifies our hiring our own programming team to write our very own software for a competitive edge. I think that the neural network our team is sketching out will really provide a tremendous boost to our data analysis capabilities for sales and also for customer support. The reason I'm writing is that I'd like you to flesh out your brief mention yesterday about defining our current system as a production system and building a new development system. Can you explain why we shouldn't just have the development team do all their work on the system where their software will ultimately run? Why should we buy and install a separate one? Oh yes, and you also mentioned separation of duties during your talk, but I don't see how that applies to the software project or is related to the new system.

FROM: Gregory Antonellis CISO
TO: Mary McDonnell, CIO
SUBJECT: re: Software Development Project

Ms. McDonnell,

In response to your questions about my presentation: A production system is a system that performs a critical function for our organization; basically, it's any system that would disrupt business as usual if it broke. A development system is a system that is as equivalent as possible to a production system but is not actually performing a task for the organization. The purpose of a development machine is to provide a safe environment to test any changes to a production machine before we make them to the production machine so that if the changes break anything our actual production machine is unaffected. Separation of duties is relevant to software development because it allows for more secure code. By having the software written and tested by different people we can ensure that there are no unauthorized additions to the code and no shortcuts were taken. We can also that testing is thorough. If the same people write and test the code there's a possibility that testing will may not be thorough if the testers assume that "we know we wrote that section right so there's no need to test it." I hope this answered your question, if not, please feel free to contact me.

Sincerely
Gregory Antonellis, CISO

* * *

3. FROM: Jamie Bamber, VP Marketing
TO: YOU as CISO
RE: Ethical problem

Hi! Mary McDonnell and Eddie Olmos both suggested that I discuss a current issue with you because, they said, you come from a university with strong emphasis on ethics. Here's the scoop: Jamila is working on a new advertising campaign to counter the most recent release of Yontraubon Industries' GzornoGood™ gzornoplatzes. As you know, we've been neck-and-neck with that company for the last six years in the same market, and our GreatGzorn product really needs a marketing boost. Well, it turns out that Jamila's boyfriend's sister's husband works at Yontraubon as a Senior VP of Marketing and is really irritated at the way he's been treated in the last year. He was supposed to get a major account from his boss but instead his boss gave the account to the boss' own mistress!! Isn't that appalling? Anyway, this guy is ready to jump ship and join our company right away – and the best thing is that he is willing to bring us inside information about the next generation of GzornoGood™ gzornoplatzes! With that information, which includes some schematics and test data, we can get our own GreatGzorn's out by next September with even more features and at half the cost (since we won't be paying for the research and development that went into the GzornoGood™ plans). I was all set to go with this move, but Mary and Eddie said I really should ask you for your analysis of the ethical issues. I hope you can have your response ready within a day or too, 'cause we're really hot to trot here!

TO: Jamie Bamber, VP Marketing
CC: Jamila _lastname_here_
FROM: Gregory Antonellis, CISO
Subject: **URGENT:** Ethical problem

Mr. Bamber,

If we were to acquire intellectual property information via his insider knowledge it would be highly unethical and potentially illegal depending on the intellectual property involved. I recommend that we do not accept any proprietary information from this guy. I also recommend that we do not make any effort to contact this person. If he's so willing to jump ship so readily he could pose a risk to our company as well. Please tell Jamila that she shouldn't under any circumstances accept insider information her "father's brother's nephew's cousin's former roommate" (or whatever the relation is). Unless legally or ethically required to do otherwise, we should NOT follow up on this and ignore any correspondence from this individual if he does contact us. Considering that my knowledge of this situation is limited to what you emailed to me, I would recommend not yet turning him in to the management at Yontraubon Industries. I believe that's the "safest" move for all parties right now, seeing as it's possible that he's all talk. If it turns out he is actually willing to put his money where his mouth his he should be able to sink his own ship without our help. As I said, my knowledge of this situation is limited to what was in your email. Please keep me up to date on any developments.

Sincerely,
Gregory Antonellis, CISO

* * *

4. FROM: Tricia Helfer, HR Director
TO: YOU as CISO
RE: Telling us what to do in our own email

I'm sorry to tell you that your memorandum about changes in our email policy are not going over very well with many of the older employees. I've received complaints with the following criticisms, and I need your expertise to explain to these people why you are acting as you are:

- *Why are you telling us that all our corporate email can be examined at any time, for any purpose, by authorized personnel in the IT and the Security groups? Surely our email is our own, even if it's on the company servers?*
- *What's wrong with using old email messages as a way of starting new conversations? You just haul up an old message and hit REPLY ALL – simple, no?*
- *Why have you written that "Operationally significant and urgent information must NOT be consigned to email, or if it is, deliver must be confirmed in-person, by telephone conversation (not voicemail), or real-time instant messaging."*
- *Why can't our employees decide what email to delete without having to consult some sort of policy documentation? What's wrong with just keeping and deleting what our users – they are the experts in their own area, you know – feel should be kept or deleted?*

FROM: Gregory Antonellis CISO
TO: Tricia Helfer, HR Director
SUBJECT: re: Telling us what to do in our own email

Ms. Helfer,

I understand that you've received several common complaints about the revised email policy for which you would like explanation. I've copied the questions from your original email and included an answer below each.

- Why are you telling us that all our corporate email can be examined at any time, for any purpose, by authorized personnel in the IT and the Security groups? Surely our email is our own, even if it's on the company servers?

Company email is reasonably analogous to company letterhead, as communications made with company resources with company branding it is company property, not personal property. As company property, authorized personal need to be able to access it if necessary. If employees would like to use email for personal purposes they should use personal email (provided such use is in compliance with company policy) but should be aware that their use of personal email via the company network or company owned hardware, while still their property, is less private than if they were to do so using their own hardware and resources.

- What's wrong with using old email messages as a way of starting new conversations? You just haul up an old message and hit REPLY ALL – simple, no?

There are two reasons this is not correct. If one simply replies to an old message when starting a new conversation the subject line will not reflect the subject of the new conversation. Furthermore, it would be inappropriate to carry out an important email exchange (e.g. a discussion about product design) in reply to an email with a less critical topic (e.g. trading company furniture) and vise-versa. If done repeatedly, recipients quickly learn to ignore the subject line. This can cause important information to be ignored on the premise that the subject has nothing to do with the message. Secondly, the REPLY-ALL feature should only be used when every person needs to be direct recipient of an email. It is not a catch-all replacement for the proper use of the CC and BCC fields. Over use of REPLY-ALL quickly leads to the intended recipients of email disregarding messages on the premise that they are not actually of relevance. Replying to old messages with REPLY-ALL combines the effects.

- Why have you written that "Operationally significant and urgent information must NOT be consigned to email, or if it is, deliver must be confirmed in-person, by telephone conversation (not voicemail), or real-time instant messaging."

Operationally significant and urgent information mustn't be consigned to email unless delivery is properly confirmed because, **just like physical mail** there is no guarantee that the recipient will check their mail, open it, actually read it, pay attention reading it, all in a timely manner.

- Why can't our employees decide what email to delete without having to consult some sort of policy documentation? What's wrong with just keeping and deleting what our users – they are the experts in their own area, you know – feel should be kept or deleted?

I truly understand the inconvenience of this policy, but it simply is not in our control. In order to comply with various laws, standards and regulations involving healthcare, product liability, protection of intellectual property, accounting and taxes we are required to keep various types of information and the relevant communications (e.g. email) about that information for various lengths of time. I understand that our employees generally know what should be kept or deleted (as you said, they are the experts in their own areas), but we are legally required to comply with regulations regarding data storage and disposal. Please be assured that the IT dept. isn't making everyone's lives harder on a whim, we'd just rather not see steam come out of some bureaucrat's ears for not doing so.

I hope I have answered these questions in a way that's adequate for your use. If you have any further concerns please feel free to contact me.

Sincerely,
Gregory Antonellis, CISO

* * *

Notes from Prof Kabay about the Author: *Gregory Antonellis<mailto: gantonel@student.norwich.edu > is from Massachusetts and is enrolled in the Bachelor of Computer Security and Information Assurance (BSCSIA) program at Norwich University. He entered Norwich with Advanced Placement College Board courses in Calculus, General Physics I and General Physics II. He already has extensive experience in programming and was exempted from taking the introductory first-year programming courses, going directly into second- and third-year courses in his first semester. He took five courses instead of the required four in his first semester, and is taking six courses instead of the required five this semester. I am proud of how Norwich University supports our gifted students and expect to see Mr Antonellis contributing significantly to our field. Anyone interested in offering Mr Antonellis internships is welcome to contact him directly!*

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *