

~~SECRET~~**Out of Control (U)**

(b)(3)-P.L. 86-36

INTRODUCTION (U)

(U) In their quest to benefit from the great advantages of networked computer systems, the U.S. military and intelligence communities have put almost all of their classified information "eggs" into one very precarious basket: computer system administrators. A relatively small number of system administrators are able to read, copy, move, alter, and destroy almost every piece of classified information handled by a given agency or organization. An insider-gone-bad with enough hacking skills to gain root privileges might acquire similar capabilities. It seems amazing that so few are allowed to control so much – apparently with little or no supervision or security audits. The system administrators might audit users, but who audits *them*? Even if higher level auditing of system administrators takes place, it is unlikely that such audits are frequent enough or extensive enough to be effective, especially against experts who probably know their systems better than their auditors.

~~(S UO)~~ This is not meant as an attack on the integrity of system administrators as a whole, nor is it an attempt to blame anyone for this gaping vulnerability. It is, rather, a warning that system administrators are likely to be targeted – increasingly targeted – by foreign intelligence services because of their special access to information. This is especially true for the system administrators of classified networks. Historical evidence of foreign intelligence targeting of U.S. communicators – people who had special access to cryptographic material – strongly supports this assertion.

(U) This situation also raises a concern about individual accountability for classified information. In short, individual users have lost control over access to electronic versions of their classified files. If the next Aldrich Ames turns out to be a system administrator who steals and sells classified reports stored on-line by analysts or other users, will the users be liable in any way? Clearly, steps must be taken to counter the threat to system administrators and to ensure individual accountability for classified information that is created, processed, or stored electronically.

**COMMUNICATORS HAVE BEEN HEAVILY TARGETED
FOR THEIR ACCESS TO KEY ~~(S UO)~~**

~~(S UO)~~ During the Cold War, untold numbers of people were recruited by Soviet Bloc intelligence services to spy against the U.S. and the West, but among the most prized agents were U.S. communicators or others who could supply cryptographic material and related information. Between 1946 and 1986, at least seventeen U.S. government

~~SECRET~~~~U.S. ONLY ORCON~~

~~SECRET~~

CRYPTOLOGIC QUARTERLY

personnel were known to compromise U.S. cryptographic systems on behalf of foreign intelligence services, primarily those of the Soviet Union. [redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

SYSTEM ADMINISTRATORS ARE POTENTIALLY MORE LUCRATIVE HUMINT TARGETS THAN COMMUNICATORS (S-~~UO~~)

~~(S-~~UO~~)~~ With system administrators, though, the situation is potentially much worse than it has ever been with communicators. In part, this is because the system administrators can so easily, so quickly, [redacted] steal vast quantities of information. Communicators of the past usually sent only relatively short messages and "finished" documents, but today's system administrators can obtain full-length copies of entire reports, including draft versions, as well as informal e-mail messages, electronic calendar appointments, and a wide variety of other data.

~~(U)~~ [redacted]

FOREIGN INTELLIGENCE SERVICES ARE ALREADY TARGETING COMPUTER PERSONNEL (S UO)

~~(S-~~UO~~)~~ It is their tremendous access to classified information and their control of classified computer systems that make system administrators prime targets for foreign intelligence recruitment. [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[redacted]

It is their tremendous access to classified information and control of classified computer systems that makes system administrators prime targets for foreign intelligence recruitment. (S-~~UO~~)

~~SECRET~~

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~(S U O C)~~ [Redacted]

~~(S U O C)~~ The KGB's handling of the German Hanover Hackers was one of its earlier efforts in the computer hacking arena and was made famous in Cliff Stoll's book *The Cuckoo's Egg*. The hackers provided passwords, logon account identifications, source code and other information for unclassified U.S. government computer systems. The KGB, however, considered the case a disaster because the hackers were unreliable and ended up exposing the whole operation. For the KGB, it was a learning experience, and by 1991 they were using the case as an example of how *not* to run an operation. The implication is that their Russian successor organization, the Russian Foreign Intelligence Service (SVR), is now more likely to target insider computer personnel rather than hackers. Of course, this does not prevent them from accepting "walk-in" volunteers or using their own intelligence personnel to "hack" into systems directly.

... just as unbreakable U.S. cryptography has pushed foreign intelligence services to target the people who control the key, so too will stronger network security spur increased targeting of the people who control the computers.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~(S U O)~~ [Redacted]

The continuing increase in general computer exploitation efforts suggests, however, that it is only a matter of time before successful computer personnel recruitments are discovered.

~~(S U O)~~ This warning about the HUMINT vulnerability is in no way meant to downplay the need for stringent technical security solutions, but just as unbreakable U.S. cryptography has pushed foreign intelligence services to target the people who control the key, so too will stronger network security spur increased targeting of the people who control the computers.

~~SECRET~~

CRYPTOLOGIC QUARTERLY

THE NEED FOR MORE INDIVIDUAL ACCOUNTABILITY (U)

(U) This threat highlights the need to control classified electronic files, but, as most users of classified client-server networks already know, individuals have far less control over their own classified electronic files than they have over their hard copy documents. In short, people are doing things with electronic copies of classified information that would never be allowed with paper. For example, if a file is sent to the printer and does not print out, it is assumed to be a "glitch" - not a "lost" copy of a classified report.

(b)(3)-P.L. 86-36

~~(FOUO)~~ In one incident at NSA, highly classified material printed out after hours on the wrong printer in the wrong room and was turned in by the cleaning crew! In another incident at NSA, a large number of files sent to a printer at different times by different personnel in one office mysteriously ended up in the queue of another office's printer. The files were presumed "lost" as a result of some unknown glitch and were not recovered until the user of the other office's printer came back from TDY and turned the printer on. This was not a simple case of using the wrong printer name; [redacted]

[redacted] There have also been many other incidents in which files sent to printers never print out or print out months after being sent.

~~(FOUO)~~ Such problems, however, are not always accidental. In 1994, for example, a contractor employee at a Regional SIGINT Operations Center (RSOC) was caught accessing restricted files on a classified system. In another incident at the same RSOC, three

[redacted]

From an individual's standpoint . . . access to electronic versions of classified documents is out of control.

(b)(3)-P.L. 86-36

~~(FOUO)~~
(U) These mysterious glitches and insider abuses demonstrate how difficult it can be to control electronic files. With hard copy, classified files are locked away in safes or desk drawers or cabinets when no one is around to keep an eye on them. Even when they are open during the day, access to any particular room is limited to only certain people. Does this mean that all individuals have perfect control over their hard copy documents? Of course not. [redacted]

[redacted]

[redacted] Nevertheless, access to classified hard copy is, in general, still controlled by the people who are responsible for it.

~~(S)~~ From an individual's standpoint, however, access to electronic versions of classified documents is out of control. Intelligence personnel can no longer lock the draft versions of their Top Secret SCI reports in their safes at night and go home feeling reasonably secure. Instead, those reports and almost everything else they have done is out of their control, stored electronically on some server in some other room or even in another building. Now

~~SECRET~~

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

OUT OF CONTROL

~~SECRET~~

when they go home at night, some of them are undoubtedly plagued by questions that all intelligence personnel should ask themselves:

Exactly how many copies of my computer files exist at any given time (including back-up files and tapes)?

Where are those copies physically located?

How many people other than me have legitimate access to my computer files, who are they, and do they have the proper clearance and the need to know?

How many people have illegitimate access to my files, either through malicious actions or unintentional error?

When I send a file to the printer or over e-mail and it doesn't make it, is the information originally sent destroyed? Stored in a buffer? Printing out on some unknown printer in another office? Or has it been captured by an insider hacker?

If the next Aldrich Ames turns out to be an NSA system administrator, and he steals and sells copies of my classified computer files, will I be liable in any way?

(U) These are troubling questions because, even though the vast majority of intelligence personnel are not system administrators, they are still legally, professionally, and morally responsible for the classified information that they produce, handle, or store. Users of classified systems must, therefore, be given greater control - individually - over the electronic versions of their notes, reports, and other documents. The information at risk includes

widely disseminated classified and sensitive-but-unclassified documents;

highly compartmented information with very strict need to know;

information protected by the privacy act, such as personnel files, medical records, and security files;

other highly sensitive information, such as Inspector General investigations and security investigations for counterintelligence or law enforcement matters.

CONCLUSIONS AND RECOMMENDATIONS (U)

~~(S)~~ The growing threat to system administrators heightens the need for accountability for classified electronic information, but there is no one easy answer to this problem. Most users enjoy and appreciate new technology and all of the associated benefits, from e-mail to bulletin boards to Web browsers to cost-saving shared resources. It is unlikely that anyone wants to return to the pre-client-server era, even if it were possible to do so. Still the military and intelligence communities must do *something* if they are to reestablish

~~SECRET~~

CRYPTOLOGIC QUARTERLY

individual employees' control over the information for which they are personally responsible. Possible actions include the following:

~~(U//FOUO)~~ ~~(S//FO)~~ *Intensify counterintelligence scrutiny of system administrators. This is*



(U) Allow physical separations from networks. Allow each workstation to function as both a stand-alone and a network terminal, with a physical disconnect from the LAN or other network. People who need to work on highly sensitive matters could thus do so with less anxiety about network attacks by physically disconnecting from their LAN. To be effective, this would require the more expensive installation of word processing or other applications on each workstation – rather than as a shared network resource using “licenses” – but it would also allow people to be productive during network down time. Of course, connecting to the network to send e-mail or surf the Web would have to be a relatively quick and easy procedure – such as plugging in a cable and then clicking on an icon.

~~(FOUO)~~ *Provide encryptable hard drives. Analysts and managers should be able to store information on their own workstations' individual hard drives in an encrypted form that cannot be decrypted by anyone else, including system administrators. Yes, some people will forget a password or something and end up losing an important file, but that is the price of individual responsibility. Those analysts who do highly compartmented or otherwise sensitive work should be provided with removable hard drives that can be encrypted and stored in a three-combo safe. It would be preferable if, in the future, all hard drives could be removed for storage in a safe to prevent theft or damage from fire or other disasters. But then exit inspections would have to be reinstated to help prevent people from carrying the drives out. An alternative would be to install sensors at each exit and tag each drive with a trigger mechanism, similar to the technology used by stores to combat shoplifting.*

~~(FOUO)~~ *Give M5 and other security organizations more money. It is unwise to cut security budgets now, and it's not only because of the threat of a specially equipped Ryder rental van taking out half of the FANX III building. Overall, employee susceptibility to foreign intelligence recruitment has probably increased in this era of unprecedented budget cuts and the accompanying low morale. In the long-term, security acts as a force-multiplier because it limits*

~~SECRET~~

OUT OF CONTROL

~~SECRET~~

otherwise exponential losses caused by spies, and good budget planners know that force multipliers should not be cut at the same rate as regular forces during downsizing.

(S) These proposed measures would be expensive, but they are necessary given the growing foreign HUMINT threat to system administrators. Yes, it is less expensive and far more convenient to store everything on servers, but just because it can be done does not mean that it *should* be done. If individual computer users are going to be held accountable for the classified information that each personally handles, then they must have more control over how and where their information is stored and who has access to it.

(b)(3)-P.L. 86-36

	<p>(FOUO) [redacted] is an intelligence analyst in the ISSO's Threat Analysis Division (V52). He is the primary editor of the <i>National INFOSEC Intelligence Review</i> (NIIR), published aperiodically by V52, and the <i>ISSO Global Threat Summary</i>, a reference manual also published by V52. He joined the Agency in 1986 and was professionalized as an Intelligence Research (IR) Analyst in 1990 after graduating from the IR intern program. [redacted]</p>
	<p>[redacted]</p>
<p>holds memberships in the National Military Intelligence Association, the Association of Old Crows, and the International Affairs Institute. He was formerly a chapter president of Pi Sigma Alpha, the National Political Science Honor Society. He is an award-winning essayist and has published several articles in professional journals at NSA and CIA.</p>	

(b)(6)

Derived from: NSA/CSSM 123-2,
Dated 3 September 1991
Declassify On: Source Marked "OADR"
Date of Source: 3 Sep 91