

Security Lessons Learned from Société Générale

“The sign above the players’ entrance to the field at Notre Dame reads ‘Play Like a Champion Today.’ I sometimes joke that the sign at Nebraska reads ‘Remember Your Helmet.’ Charlie and I are ‘Remember Your Helmet’ kind of guys. We like to keep it simple.” —Warren Buffett

The financial news of early 2008 has been dominated by the continuing credit crunch in the US and elsewhere, but for sheer drama, the loss of nearly €5 billion (roughly US\$7 billion) in

Security professionals are familiar with this problem because it’s one of the oldest in the book. Any of the well-known solutions (such as use of one-time passwords, tokens, biometrics, or smartcards) would have avoided it, but only if Société Générale employees didn’t just leave the token or smartcard on their desks. Coupling a better authentication scheme with improved user security awareness might have been enough.

Lesson 2: *Logs are only useful if they’re examined*

Reportedly, the bank had adequate logging systems, so it might have caught the problem sooner. However, it’s well recognized that having logs and looking at them are two different things—ditto having the tools available to make digging through those logs feasible. Logs that show operating-system- and network-level activity are relatively useless in detecting the sort of failure Kerviel introduced, as are intrusion detection systems operating at low levels. Instead, application-level logs and intrusion detection systems are critical because they can focus on detecting unexpected transactions and patterns, which narrows the field considerably.

Our lesson learned here is that intrusion detection systems must operate where the activity occurs, not just focus on the well-understood network and operating sys-

JEREMY
EPSTEIN
*Cyber Defense
Agency*

unauthorized transactions by trader Jerome Kerviel at French bank Société Générale is far more exciting.

The story is still unfolding as of this writing, and Kerviel hasn’t yet been convicted of any crimes, but the news coverage indicates that he used his knowledge of how the trading system was managed (gathered in a previous position in the bank) to go undetected for at least two years. Initial claims stated that he was a “brilliant” technologist who subverted controls by hacking bank computer systems, but these claims seem to have been incorrect. Instead, it appears that he succeeded by understanding how to stay under the radar. Security professionals tend to be “remember your helmet” people, so it’s worth learning from the failures.

Lesson 0: Measure the right risks

On 15 February, Bloomberg News quoted an analyst who summed it up best: “Risk control was too oriented toward market risk, at the expense of operational risk and

fraud risk in trading activities.” The infamous TJX case offered a similar lesson, with management more concerned about reputational risk (that is, will people refuse to buy from TJX-owned stores) than the operational risk from weak credit-card controls. In the TJX case, this appears to have been the right decision: although the security community wrung its hands over the company’s sloppy security measures, TJX’s sales and stock price have continued to increase, despite the theft of personal information about millions of customers.

Lesson 1: Low tech attacks are easier

Despite early reports, this attack was decidedly low tech. Kerviel stole or guessed other traders’ passwords and used them both to spread and approve his actions, a clear violation of the separation of duties. How he stole the passwords hasn’t yet been explained—was it poor password choice, user password sharing, repeated password guessing, or something as simple as a yellow sticky taped to a monitor?

tem levels. Such systems should take into account not only what happened, but when: use of a trader's ID outside his normal work hours was a missed clue (Kerviel apparently used other traders' accounts after hours). As noted in lesson 0, ignoring factors such as the time of the event is missing the risk. Integrated logging should also include physical activities such as entering and leaving secured areas.

Lesson 3: Don't rely on secrecy for security

Auguste Kerckhoffs' principle from the late 1800s states that "only secrecy of the key provides security," or as Claude Shannon restated in the 1940s, "the enemy knows the system." Claims that Kerviel succeeded because he knew the security system's secrets might be true, but if they are, they indicate that the system wasn't properly designed in the first place. A Security Management News blogger wrote, "the fact that Kerviel may well have used his IT background to help carry out the fraud highlights the need for special controls to be in place for internal employees who move from one controlled team to another" (www.exaprotect.com/resources/newsletters/societe-generale-losses-provide-lessons-for-us-all). Security professionals would (or at least should!) disagree with a secrecy-based approach: security systems must be designed so that even if the attacker (in this case, the rogue trader) has complete information about how the security system functions, it still operates successfully.

Lesson 4: We're looking at the wrong things

The security industry in general and most security researchers in particular are far more concerned

with preventing attacks by malicious users and phishing scams that subvert innocent users than they are with insider attackers. In fact, relatively little research, and even fewer solutions, exists for such attacks. Organizations tend to focus on the threat itself rather than on protecting assets, which clearly leaves the entire system vulnerable.

Lesson 5: Rights revocation must be tied to role assignments

Some reports indicated that when Kerviel transferred from a back-office job to a trader's role, the bank added new access rights but didn't remove the old ones. This might have allowed him to perform actions such as approving his own activities (see lesson 1) and reviewing logs to see which of his activities were drawing attention (see lesson 2). Role-based systems tend to make it easy to add new rights but relatively less straightforward to remove them—yet role aggregation can allow unanticipated escalations. We should also consider the human interface factor as a lesson learned: perhaps role-based systems should explicitly ask an administrator if roles are to be removed when new roles are added, instead of relying on the administrator to remember to make that change without prompting. This isn't a flaw in role-based access systems but rather in how they're managed.

Lesson 6: Social engineering is a threat

Management was all too willing to accept Kerviel's explanations of unusual activities. According to press reports, Société Générale had begun investigations his activities months or even years before he was caught, but he was able to explain away suspicious activities. It's a natural human trait to want to believe someone's explanation, and being too skeptical can destroy

workplace morale. But especially in a high-stakes environment such as a financial institution trading floor, management should follow the maxim to "trust but verify."

Lesson 7: Don't believe everything you read

Kerviel allegedly covered his tracks by sending forged emails to approve his own actions—management simply wasn't aware or chose to ignore the fact that the "from" address on an email isn't necessarily authoritative. I'm reminded of a true story in which a small company president started to celebrate when he got an email from `president@whitehouse.gov` informing him that his company had received a substantial grant. Even though he was technically astute enough to know that it could have been forged, in his excitement and desire to believe, he forgot. Perhaps management at Société Générale was excited by Kerviel's purported successes and forgot that they shouldn't blindly believe everything they read. Thankfully, this is one of the easier problems to solve, if digitally signed email is deployed. (But even so, many technical users don't realize that S/MIME and PGP don't sign email message headers, so they can't always rely on "from" addresses even for signed email.)

Lesson 8: Cutting staffing costs can backfire

The International Herald Tribune reported that "central bank officials had previously warned Société Générale that its risk-control departments were insufficiently staffed" (www.iht.com/articles/2008/02/20/business/socgen.php). It's not unusual for companies to skimp on risk management because it's a cost center rather than a profit center. But as Société Générale has painfully learned, that's a false economy.

Lesson 9: Features without assurance are ineffective

We have yet to learn what mechanisms were in place at Société Générale for determining whether fraud detection was effective, even to the extent that such mechanisms might have been incomplete. Did the bank test to see that its logs had the correct information, that authentication failures were logged, and that processes were in place to review those logs? Preliminary findings indicate that the technical measures generally operated correctly, but the human processes to follow up on them were deficient (www.theregister.co.uk/2008/02/21/socgen_probe_latest). Management approval of technology solutions should therefore also include review of the corresponding human processes.

Lesson 10: What's happening behind the scenes

Security in business is like sausage: you don't want to see it being made. Mapping arcane general-purpose security products, protocols, and processes to real-world business systems isn't an exact science. Our security primitives are hard to use and need better tooling to help business people make reasonable decisions. Lessons 5 and 7 are especially relevant to this point.

Non-lesson 11: Insider attacks (usually) have motivation

The intelligence community has long used nontechnical measures—such as seeking to determine if individuals have political or financial motivations—to help it find spies. This technique is applicable as well to financial and other institutions, and many organizations use periodic person-

nel background checks to help detect insider risks. However, Kerviel didn't seem to be motivated by personal financial gain or a desire to damage his employer or markets. His motivation remains a mystery, so we can't yet claim any lessons learned in this area (although it's certainly something to consider as part of a security posture).

Non-lesson 12: Security measures are useless if they're turned off

Unlike Société Générale, MF Global's US\$141 million trading loss, which was revealed as this article was going to press, had a simple explanation: "the firm had deactivated [the controls] for certain traders [...] because the controls slowed transactions" (www.iht.com/articles/2008/02/29/business/29trader.php). Whether MF Global's management understood the wisdom of disabling such controls hasn't yet been revealed. The controls might have prevented the loss, but as the US nuclear industry recently learned, a sleeping security guard is the same as no security guard at all.

We can blame Société Générale's loss in part on technology failures, but learning from what went wrong and recognizing the limits of technology are critical to avoiding future failures. It's our duty to design both technological and nontechnological processes to prevent and detect unauthorized actions by insiders. □

Jeremy Epstein is a senior security consultant at the Cyber Defense Agency. His technical interests include security of service-oriented architectures and voting systems. Epstein has an MS in computer sciences from Purdue University. Contact him at jeremy.epstein@cox.net.