


Good morning. My name is Patricia Ensworth. I'm a business anthropologist based in New York City. I lead a consultancy that provides services for project management, requirements definition, and business analysis. Most of my clients are software engineering and information technology groups at large global organizations in the financial services industry. I'm also a faculty member of the American Management Association.

I'm here today to bring you a report from the field. Our topic is "Web 2.0 and Information Security: Challenges for Corporate Ethnography."

## Agenda



- Recent changes in corporate environment due to security issues affecting end-users
- Impact of changes on ethnographic data-gathering methods and tools
- Recommended responses to changes by ethnographers analyzing work practices


I will be talking about recent changes in the work environment that have affected the validity of research methods employed by ethnographers who study work practices, work processes, and organizational behavior.

The changes are part of a trend that is already well underway whereby what we call “work” is increasingly disembodied and invisible because it is based upon data transactions.

Under these circumstances, we ethnographers should step back and re-evaluate our methodologies.

We should also appreciate that this situation creates an opportunity for us to demonstrate how our approach and expertise can be quite valuable.

## Web 2.0 within organizations



- Virtual community
- Content creation
- Co-authoring activities
- Shared resources
- Behind the firewall
- Value added to business

Let's begin by defining our terms.

“Web 1.0” describes the first phase of the internet where the World Wide Web delivered only pre-packaged content to passive digital consumers. “*Web 2.0*” describes the current environment where users form virtual communities to create content together through collaborative co-authoring with shared resources. In the personal domain, most of us are familiar with social media sites such as Facebook and LinkedIn; other examples would include gaming platforms, recreational listservs, blogs and wikis.

In a corporate environment, “Web 2.0” would refer to similar activities behind the organization’s firewall that added value to the business. For example:

- A credit rating agency’s workflow system where different analysts discussed their opinions of a new investment product.
- A knowledge management system or project Sharepoint site.

All of these would illustrate Web 2.0 principles.

Security incidents 2010-2011



- Aurora
- WikiLeaks
- Stuxnet
- RSS Secure ID
- *News of the World*

↓

**"We don't trust our internal networks"**

How many of you in the audience have:

- Had your e-mail account hijacked and spam sent to people in your address book?
- Accidentally downloaded a virus that destroyed your files?
- Been the victim of identity theft and received calls from credit bureaus asking why you had charged lots of merchandise you hadn't actually bought?

In layman's terms, *information security* is the condition in which none of these problems ever occur.

During the past two years, the information security challenges faced by corporations have increased dramatically.

The event that launched this new era occurred in January 2010 when news reports disclosed that hackers in China had broken through the firewalls protecting Google's servers and had stolen source code for their search engine. This was a serious problem for three reasons.

First, in the realm of business it amounted to a successful theft of intellectual property, akin to a beverage competitor stealing the secret formula for Coca-Cola.

Second, in the context of the ongoing conflicts between the U.S. and China over trade and human rights, it represented an act of cyberwarfare: by picking the digital locks of an important American high-tech company, a rival nation-state had laid bare the weaknesses of our cyberdefense strategy.



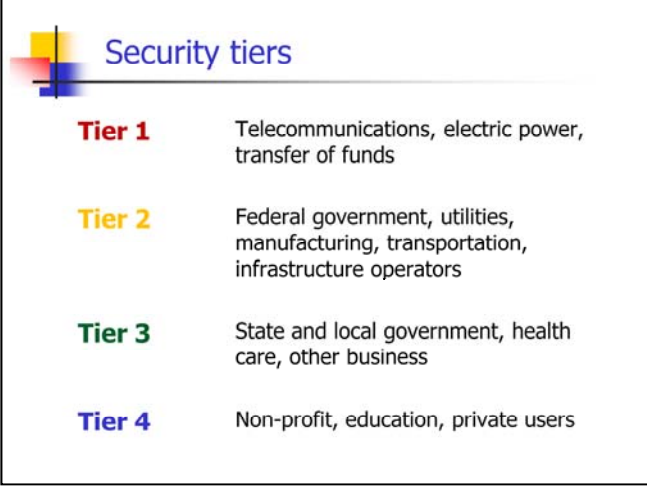
Most important, the national security implications were potentially dire. Many organizations have incorporated elements of Google's source code into the search features of their own intranets. If hackers could break through those organizations' firewalls, in theory they could execute the commands in the stolen source code, snoop around, copy data, take control of systems, and generally wreak havoc.

Soon after Google revealed the theft, federal agents contacted organizations considered critical to national security and ordered senior management to inspect their systems, remove any malware they found, and fortify their IT defenses. To accomplish these tasks – collectively called Operation Aurora – most organizations appointed a special project manager.

In February 2010 I was recruited as a consultant by a global investment bank to manage their Operation Aurora project for one year. My experiences during this engagement provided the motive and the primary source material for this paper.

It soon became clear that the Aurora cyberattacks were not an isolated incident. As the year progressed, there were other high-profile cases. Next came the WikiLeaks that targeted U.S. military foreign policy data. Then the Stuxnet worm that targeted Iranian nuclear operations data, followed by the RSS break-in that targeted identity encryption data, and the *News of the World* mobile phone network hacking that targeted voice mail data.

Ultimately, the net result was a realization that the information traveling on many organizations' internal networks inside the firewall was considerably less secure than management had believed.

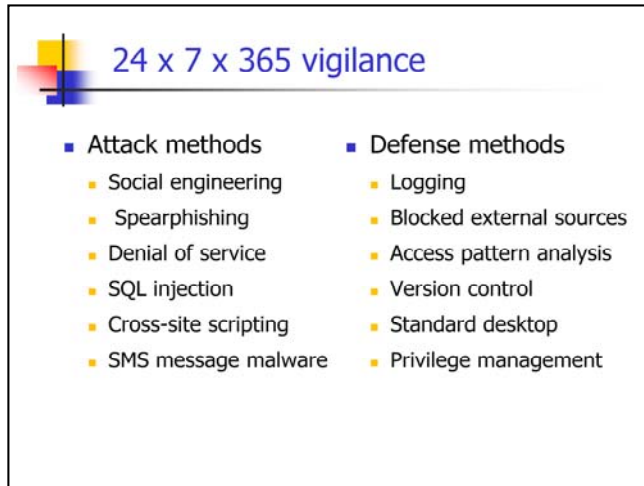
A diagram titled "Security tiers" enclosed in a black rectangular border. The title is in blue text at the top left, next to a small graphic of overlapping colored squares (yellow, red, blue). Below the title, four tiers are listed, each with a colored header and a list of associated sectors. Tier 1 is red, Tier 2 is yellow, Tier 3 is green, and Tier 4 is blue.

Security tiers	
<b>Tier 1</b>	Telecommunications, electric power, transfer of funds
<b>Tier 2</b>	Federal government, utilities, manufacturing, transportation, infrastructure operators
<b>Tier 3</b>	State and local government, health care, other business
<b>Tier 4</b>	Non-profit, education, private users

To put the issue in perspective, the degree of danger varies based upon the sector of the target organization.

Both the European Union and the United States Commissions on Critical Information Infrastructure Protection agree that three civilian sectors are of paramount importance to the operation of society: telecommunications, electric power, and transfer of funds.


However, there is a trickle-down effect to other sectors – and a desire among Chief Information Officers to demonstrate that they are alert watchdogs. It is expected that stricter protocols will soon be adopted in some degree by most organizations.



Depending upon external political and economic factors, a Tier 1 global organization with 50,000 workers can expect between 100,000 and 200,000 hacker attacks every day. All but a few dozen are blocked by the firewall. The more sophisticated types – some of which are listed on the left of the slide – require the Computer Emergency Response Team to spring into action and perform damage control.

To reduce the risk from a variety of attack methods, IT Security groups have implemented stronger defensive tactics across the organization.

- All user behavior is logged. This includes every hardware platform: Windows, Unix, mainframe, telecommunications.
- Downloading files is forbidden. USB drives are disabled. Connections are blocked to websites for personal e-mail, social networks, job hunting services, and other non-business functions.
- Patterns of file access are analyzed for anomalies. If you usually work with files on server X, and one day you try to open a file on server Y, it will be noted.
- Users are required to install all software security patches and eliminate end-of-life versions from the IT environment.
- Every computer desktop is required to run the same standard software installed from a master “gold build.” All the programs on the standard desktop must have passed a security “penetration test” in which professional hackers try to break it. Exceptions to this rule for software engineers building new custom programs are permitted, but must be extensively documented and justified.
- Most disruptive to the organization, yet most interesting to an anthropologist, is the mass revocation of permissions to use shared IT resources. Trust relationships that are based on informal grass-roots networks of professional kinship become codified, with privileges managed by a centralized bureaucracy. Negotiations about who can do what when focus on technical interpretations of purity and danger.



### Changes in end-user behavior

- Heightened awareness of constant surveillance
- Reduction in time and resources for creativity
- Assumption of hostile audience for all written communication through the network
- Proliferation of unsupported technology
- Increase in off-network data and phone traffic
- Increase in reliance on personal connections

Inevitably, all these precautionary measures have affected the work environment. The atmosphere among Web 2.0 colleagues has changed from a friendly small town where neighbors keep their doors unlocked to a high-crime battle zone where everyone is suspect.

More than ever, workers feel they are being watched as they perform their jobs. In the past it was assumed that one would be watched if one's performance or honesty were in question, but now it is everybody all the time.

This awareness becomes more acute during budget season, when funds are diverted from innovation to fulfill security requirements.

It is now assumed that anything one writes in a document, e-mail or instant message could be leaked. Written communication then becomes less of an exchange of ideas than a transcript of a negotiated agreement.

To keep ideas flowing, workers are increasingly bringing in their own personal devices such as smartphones and tablets.

At their desks but off the company network, or on the move, people employ these personal devices to communicate with colleagues about sensitive issues via private voice messages, texts, e-mails, tweets, and social network postings. Activities such as shopping, job hunting and vacation planning can occur in private. In effect, there is now a shadow communication system.

In this climate of anxiety, workers also fall back upon their own network of trusted professional connections to get things done under the radar without written instructions.





Under these circumstances, we ethnographers would be wise to re-evaluate our methods and make some adjustments.

Analysis of archived e-mail messages to identify opinions and issues is no longer as useful because the content of the messages has been self-censored and sanitized.

Exploratory research in the digital filing cabinet is less feasible because it is likely to set off the anomalous access alarms.

Direct observation for short periods of time and self-reporting diaries may not yield valid data because people stay on the network and avoid using personal technology when they know they are being observed.

On the other hand, analysis of project artifacts can furnish unexpurgated primary source material. Meeting agendas and minutes, project plans, logs of issues and risks, change control tickets, and defect tracking entries chronicle workers' true opinions.

Within legal and ethical constraints of privacy, indirect observation has the potential to make digital work practices much more visible. User experience researchers and interaction designers employ activity logs, screenshots, browsing histories and eye tracking to show where a subject's attention is focused among the various devices and systems in the environment.



Physically shadowing an individual for multiple sessions over a period of weeks establishes a relationship between researcher and subject that gradually encourages more natural behavior with personal devices.

Whether it is called participatory design, a requirements workshop, or a quality circle, bringing colleagues together to talk about what they do and what they need enables them to voice comments that they might not commit to writing for the archive.

Ultimately the fallout from the organization's loss of trust in its internal IT network has been a decline of trust and communication among many human actors on the network. Any method an ethnographer employs that can help rebuild that trust, and reconnect members of the Web 2.0 community, earns dividends of goodwill for our profession.



**Ethnography future success factors**

-  ■ Protect sensitive data
-  ■ Understand organizational constraints
-  ■ Explain ROI of stakeholder analysis
-  ■ Make invisible work practices visible
-  ■ Enhance productivity and prosperity

Beyond adapting our methods, we should be mindful of some new factors our research subjects will be considering as they decide whether they want to work with us.

First and foremost, we have an obligation to protect *our* data about the people and organizations we are studying. If the data is stored anywhere outside the sponsoring organization’s firewall, we are responsible for its vulnerabilities. Recently I met with the head of Vulnerability Management at a Tier 1 company to review with him the key concepts of this paper. A reformed hacker, he is paid well to think like an evildoer. A few minutes into our discussion, his eyes began to sparkle. “Does this mean,” he asked, “if I hacked into an ethnographer’s database I could save myself a lot of trouble gathering information I could use for social engineering or spearphishing?” The answer is: yes. Unless we can demonstrate to our research subjects that we are well-informed about their information security needs and can defend their data from hacker attacks, the demand for our services and the access to their environment will vanish.

When we engage with our research subjects, we should understand the security constraints under which their organization and their specific team operate. A checklist should serve to establish how restricted their technology environment is and how much surveillance they endure.

For many businesspeople, the term “ethnography” still evokes images of primitives dancing around a bonfire. In the current climate of anxiety about outsiders, this is an obstacle. We can more easily gain access, establish trust, and perform our research if we re-brand our activities and leverage existing organizational procedures. The expense of our engagement is more likely to pass budget review if it is categorized under project management, requirements definition or business analysis, and if it integrates with the people, processes and tools already in place.



One persuasive argument in favor of ethnography can be presented in the project management language of stakeholder analysis. Ethnographers are especially skilled at finding, understanding and explaining vulnerable communities whose voices would not otherwise be heard. Often the cooperation and involvement of such groups are critical to a project's success – and the groups are not discovered until implementation. When members of the community engage in work practices that conflict with security policies, both the project and the organization are at risk. Ethnographers can help prevent this exposure.

In conclusion, this paper has explored how recent changes in organizations' information security defense strategies have disrupted Web 2.0 communities and increased the difficulty of studying work practices and processes.

While these developments have created new challenges for ethnographers, and will compel us to adapt our methods, they also create new opportunities for us to fill a need.

Our research techniques and our four-field education endow us with unique abilities to peer through the cloak of invisibility surrounding work nowadays. Our efforts can improve the productivity of the organization and the prosperity of the business – and the working conditions of the people who make that happen.



## Additional resources

- Lukasik, Stephen J. "Protecting the Users of the Cyber Commons." *Communications of the Association for Computing Machinery* 54:9, September 2011, pp. 54-61.
- Leavitt, Neal. "Mobile Security: Finally a Serious Problem?" *IEEE Computer* 44:6, June 2011, pp. 11-14.
- Gross, Michael Joseph. "Enter the Cyber-Dragon." *Vanity Fair*, September 2011.
- "Anonymous no more." *The Economist* Technology Quarterly, March 12 2011.
- McGraw, Gary. *Software Security: Building Security In*. Upper Saddle River, NJ: Addison-Wesley, 2006.
- Douglas, Mary. *Purity and Danger: An Analysis of Concepts of Pollution and Taboo*. London: Routledge and Keegan Paul, 1966.