







The Wiley Corporate F&A series provides information, tools, and insights to

























realize it. Why? Because we are so intimately familiar with all things cyber. Cyber haunts the backstory of most everything we do. It is invisible. Only its



# Acknowledgments

WHILE ONE person may be responsible for actually writing a book, it is by no means a solitary pursuit. Certainly that was the case with *Cyber Threat!* My thinking about the evolution of the asymmetric cyber threat has been shaped by many people whose opinions and perspectives I respect. While we do not always agree on every issue, I do believe that the big cyber threat picture is coming clearly into focus and that we agree on many aspects of the problem and the solutions. Unhesitatingly, I would say that without their contributions, this book would not have been possible. In many







her exceptional team, including Deputy General Counsel Joanne Campo, Julian W. Smith, and Maureen Tobin





continuously under a range of perfect storm-like conditions. These cyber attacks have a telling and sometimes material impact on the organization.

But which organizations? In the February 5, 2013, edition of the *Wall Street Journal*, the editorial writers remarked that "On a visit to our offices last year,





And that doesn't begin to address the systems associated with critical infrastructure and proprietary corporate information. Inside many companies, the levels of awareness and compliance are low. That's not a good combination, and it promises a bad outcome in the event of attack, attacks that have come and will continue to come.

### Threat Intensification

The threat range is diverse. That's part of the problem. It's not one country or one group of hackers, though China and the Russian Federation are indisputably behind the majority of attacks against U.S. targets. Nor is it just one company hacking into its competitor, or one entity described ge9sar9(rll10.4ef(m)sI)0(t)TJ/F9





disenfranchised, malicious employees who steal data and sabotage data,





believes the computer is locked up and secure. But then he does something quite unbelievable. He places the car keys under the door mat on the driver's side of the car and the three walk into the gentleman's club. Several hours later when they emerge, the car and the laptop are missing.

It's Friday evening, and the executive also remembers that security had advised employees that in the event of a lost or stolen laptop they should call in immediately to notify. What the executive does know is that he is going to have a hard time explaining this one, so he puts it off as long as he can. He waits until the following Monday. Bad call.

On Monday, he calls security. Security immediately sends a signal to the laptop to disable it from (hard)-147.178.178.178 (Monda)-waitsmorni(lap)8.3(ing202.3(the)-225.6(lap)





The days of social media, mobile devices, and Internet everywhere and all of the time were still ahead of us. Of course, security failed to keep pace with the technology race. Many technologists believed that all information should be accessible to all, shared by anyone and everwd aby417.61gybyes31b3122.5(d)1gynt98.8(

vg all9dooptgic(nono)((gy)-9-2.3ag) aizzoinga37c.9(a3860.2(The)38ell9pur

For several years I had the opportunity to travel around the country, addressing information security of ficers in a number of cities. Over that period I met with perhaps a couple of thousand security professionals. From one city

cannot pretend that it is "

A question that is often asked in executive social media forums is, "What













In Russia, for example, there has been an increase in legislative action to





IS NOTHING SACRED?









unlicensed money-transmitting businesses operating without meaningful government oversight or regulation, in nations not well known for financial transaction oversight and regulation. The exchangers listed by Liberty Reserve were concentrated mostly in Malaysia, Russia, Nigeria, and Vietnam.



## THE CORRUPTION FACTOR

Government corruption is always a factor when it comes to trusted transactions, ones subject to close scrutiny, and where the interests of law enforcement, consumers' rights, and information integrity are enforced. Interestingly, each of the nations noted above that hosted the exchangers recommended by Liberty Reserve received poor ratings on the Transparency International Corruption Perceptions Index of 2012. The index scores countries on a scale of 0 to 100. A zero score means that a country is perceived to be highly corrupt, while a score of 100 means that a country is perceived to be free of corruption. No country received a score of 100, though some rated very highly.

According to the index, about two-thirds of countries scored below 50, "indicating a serious corruption problem."







that many visitors will use their corporate e-mail address as the login ID and their corporate e-mail password. The visitor will assume that the password, because it does not display on the screen in clear text, is secure. In fact, it is













in key technical fields that concern the national economic lifeline and national security; and to achieve 'leap-frog' development in key high-tech fields in which China enjoys relative advantages or should take strategic positions in order to provide high-tech support to fulfill strategic objectives in the implementation of the third step of our modernization process."<sup>1</sup>





3. Biotechnology and advanced agricultural technology
4. Advanced manufacturing and automation
5. Energy technology
6. Resource and environment technology

In more detail, these include:

1. Information technology (IT):
  - Computer software and hardware technology
  - Communication technology
  - Information acquisition and processing technology
  - Information security technology

IT is the building block of the future. There is little doubt that China has sIT

seionbsemsT

technology and information acquisition (technology) 104.3esd  
 aretargetr.slbhat  
 vionkplabn ha82(h)-9-7(ully.iv2te)5-9.9(I10TD[no2te)













One reason the axis of cyber evil may be an appealing strategy in support of Project 863 is that China already denies that it launches cyber attacks against the United States, and it wants to be able to continue to do so. Attacks coming from Iran, Syria, North Korea, or elsewhere against U.S. interests make the perfect cover for China because of the poor state of relations between these nations and the United States. That these foreign powers would launch aggressive attacks against U.S. interests is all of a kind.



















ACCORDING TO THE SELECT COMMITTEE . . .

htttto more open is





It is very important to concentrate on hitting the U.S. economy through all means possible.

—*Osama bin Laden*

1 **T**hd 2 3 C ac lude 4 5 6 7 8 C ac ou 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 103





systems, and to both develop and deliver computer viruses. Sometimes they are allied with nation-states to commit a variety of crimes.

The Internet is a tool. Tools are not goals; tools are things that help build or

of capitalism at work, and create uncertainty about financial services, food, water, health services, law and order, and the other elements necessary to sustain a functioning society. But their targets are more likely to be focused. Historically terrorists have not been known to be expert hackers. But they can buy that capability and, increasingly, recruit it. The historic status quo is changing. They may target the Internet-enabled control systems of critical infrastructure.





vdita02pa

As described in my book





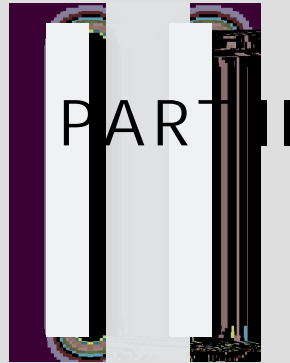


companies by causing interruptions to their operations, which could dimin-



inT

Digital Society

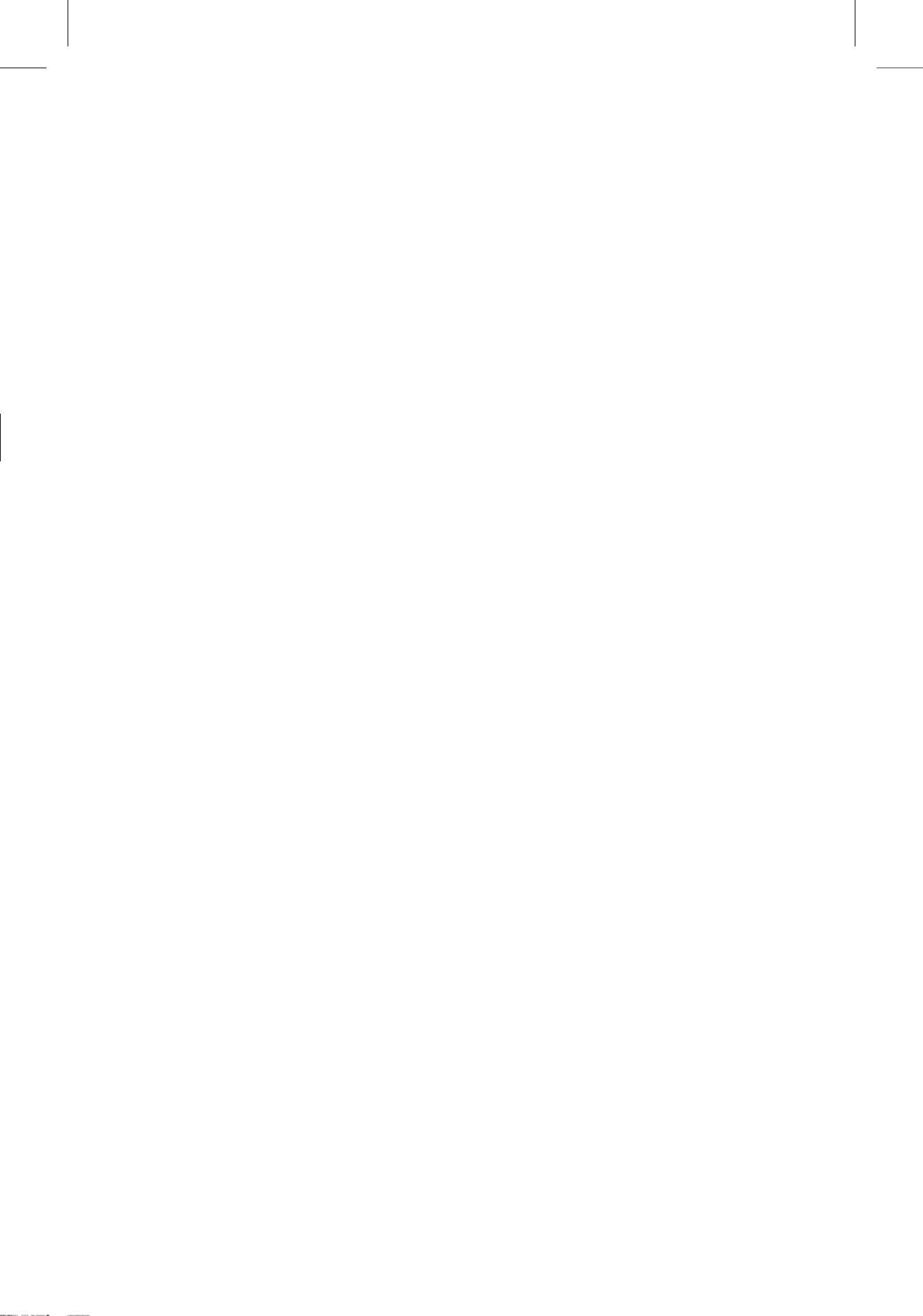


Yours















in an enterprise-wide upgrade. The company was breached over a period



Law enforcement may or may not become actively engaged. Law enforcement engagement,nt



Economic espionage is growing and has a substantial cost impact on companies in the United States and elsewhere. Many companies don't discover these thefts until months or even years later.

Here's a rational scenario: Say a company pins its financial hopes and future on a critical technology. That specific technology will be the foundation for growth, revenue, pro

behaviors, antiquated technology, ine

jobs per year from foreign economic espionage. Approximately 70 percent of cases involve insiders.

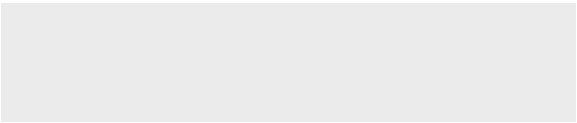
South Korea says that the costs from foreign economic espionage in 2008 were \$82 billion, up from \$26 billion in 2004. The South Koreans report that 60 percent of victims are small and medium-size businesses and that half of all economic espionage comes from China.

Japan's Ministry of Economy, Trade, and Industry conducted a survey of











Critical infrastructure is comprised of a number of sectors necessary for the country to operate under reasonably normal conditions. Here's the fundamental issue: Most critical infrastructure operations are connected to the Internet. They are therefore vulnerable. One of the problems with the executive order is that it is an executive order. On the other hand, does the nation rab0(yon)-9nnorthe 0(awson)-9.3(t)-1.1(hc)TJr nnowhellonxered?hestheionslowshe



NO GUARANTEES WITH THIS EXECUTIVE ORDER









## GOVERNMENT-INDUSTRY COOPERATION: NO SILVER BULLET

The government has not yet identi





nite(d-313139Sd)-.3tmatsd and

allsis avmatelide



The nation feared an invasion of Japan and even the loss of the war to the Empire of Japan. Americans engaged in combat were dying daily. An invasion of Japan, it was estimated, could result in a million American casualties, even in victory. Fear of more loss of life than was necessary was a powerful incentive embraced by the government that ultimately was accepted by those whose loved ones could have perished in such an invasion. There was no shortage of fear in Cold War I. Visions of nuclear mushroom clouds, delivered by inter-continental ballistic missiles (ICBMs), lled the American consciousness. The race to space would establish at least technological parity, eventually resulting



substantial numbers of utilities or others that may have not taken adequate



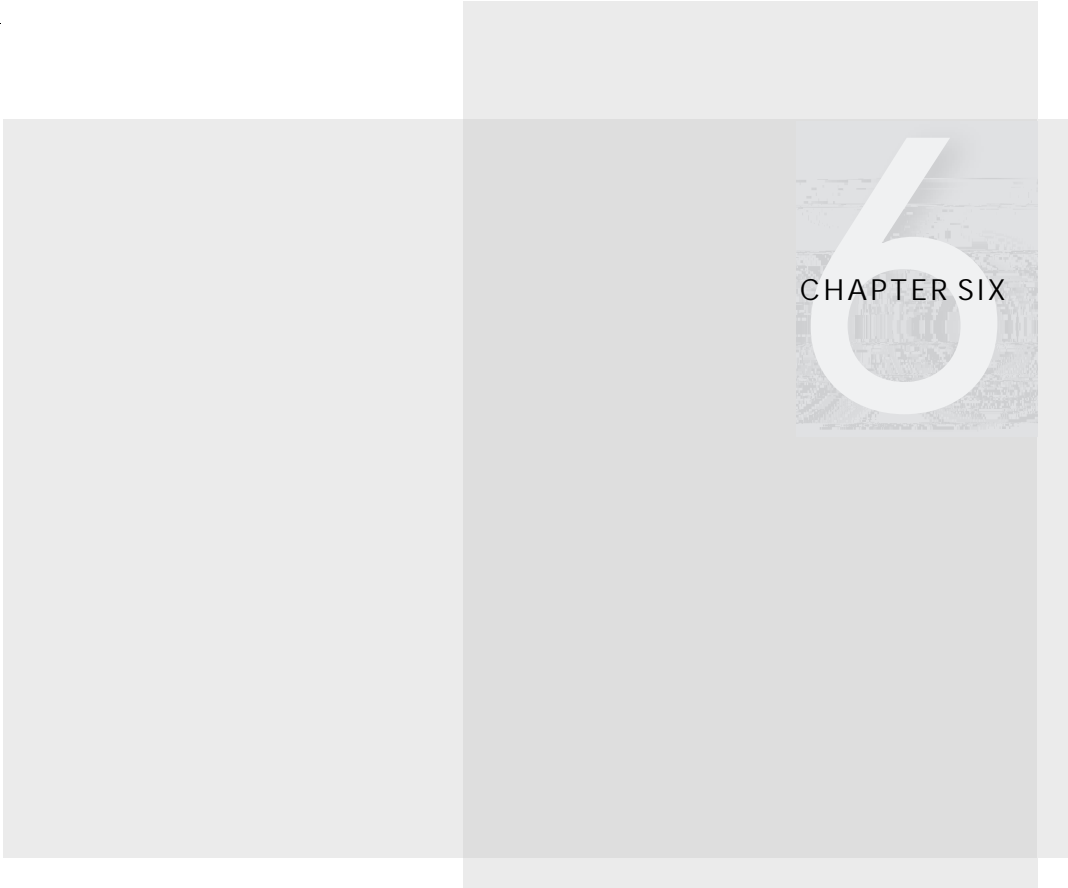
Counterintelligence means the "information gathering, and activities con-



immediacy to make this public policy. Unfortunately, there's little chance H.R. 624 or any successive legislation will pass in the Senate.

This condition is somewhat reminiscent of the days in this country leading up to December 7, 1941. Up until then, most polls showed that some 80 percent of the country had no appetite to fight Germany or Japan. Robert E. Sherwood, an American playwright and speechwriter for President Franklin D. Roosevelt, in the days leading up to that "day of infamy" observed that most Americans were more interested in the Army-Notre Dame football

Internet to provide a central fund the banks can draw on to increase their



# 6

CHAPTER SIX

table, the maitre d' came and stood before them. With a broad smile and a sparkle in his eye, he said, "Perhaps you would like to have your watch back.

It is a very ne piece." The uh3(The)-351.7(l)13(do)60(k)ed-51a(1).N(1)615354n)-1(is)-351.7(noti.017Tf()Tj36392d32740TD0T6D0Tc(308692.80T)2946.6(k30o)-72.897(wrn)29

"The growing strength of malware will expose new sources of revenue to







It's not that desktop machines were secure. It is more that they were not as

involves the rise in the U.S. workforce of different expectations regarding work,

doesn't look that way to the average user. In fact, technology has become incredibly easy to use. Tha

w41.1h



The future of Moore'













Then, in one of the more poignant moments in the lm, Billy Jack





Several trends have converged that have allowed Anonymous to lead and others to follow, creating a dangerous cyber weapon. The low cost of technology, the almost unimaginable growth of mobile devices around the world, omnipresent social media, continuous availability, and the variable degree of anonymity offered by the Internet have enabled a powerful form of protest and digital assembly.

The Web is a massive marketplace and a criminal's dream. In the case of Anonymous, the organization has confused criminal conduct with social protest. The Web has become a social rallying point, and Anonymous





"We target the bastard group that has thus far led the charge against our websites, like the Pirate Bay," Anonymous posted in an online message.

Fourteen other Anonymous members have been arrested in Ankara, Turkey, for commission of cyber crimes in numerous cities throughout that country. Their attacks were against government web sites.

The FBI has stated that Anonymous has been broken. Maybe, but that is not likely. Every time one Anonymous member is arrested, another moves in line to assume the vacated position. Anonymous has a big benc3f86.8(vent)9(houts)-367.1(that)



are filled to capacity and then overflow, ruining floors, perhaps destabilizing the electrical system. Perhaps the intruder barricades himself inside the structure,





# 8

## CHAPTER EIGHT

# Managing the Brand When the Worst Occurs

A crisis unmaskes everyone.

—Mason Cooley, professor, aphorist

C HANCES ARE,









This is especially true in the event of a breach involving regulated personal information, including medical and financial information.

valuable. Every company, regardless of size and business, should assign someone to watch over the privacy of information.

**Risk management.** Not all companies have a chief risk officer (CRO), but some do. That risk officer should always be involved and work closely with the legal of





Internal

Third-party vendors

Customers. This can be controversial since many companies under

Determine if there are multiple breach points. This is an increasingly



Personally identifying information (PPI)

Protected health information

Examine paper and electronic record formats:

Look for user-de











## CHAPTER NINE

# Managing the Big Risk

## *Third-Party Vendors*

The golden rule for every business man [or





of other organizations with the institution's processes and can increase the overall operational complexity."<sup>2</sup>

The FDIC has issued recommendations on conducting vendor due diligence, practices that all companies should commit to in examining the suitability of third-party vendors. The evaluation of a third party may include the following:

Audited financial statements, annual reports, Securities and Exchange Commission filings, and other available financial information;

Significance of the proposed contract on the third party's financial condition

TD(nanc)-8.8(ial)-337.3(inform)-8(ation;)t0r8867Tm.5g()Tj/F11Tf9.9626009.9626108

manage head count and budgets, and to contract and expand more readily in response to market reduction and growth. In the case of outsourcing, there are tremendous financial incentives to use lower-cost resources. The use of offshore third parties has become so widespread that a few years ago one venture capital





parties, but too frequently the process of determining the risk associated with hirde

parly

regulatory minimum requirements for information protection and breach







Federal Information Security Management Act (FISMA), is an excellent guideline. Many private-sector organizations use many elements of NIST



- i. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
- j. Monitoring and enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Define information privacy for the vendor, and how it must be observed and managed. Information privacy is about how regulated



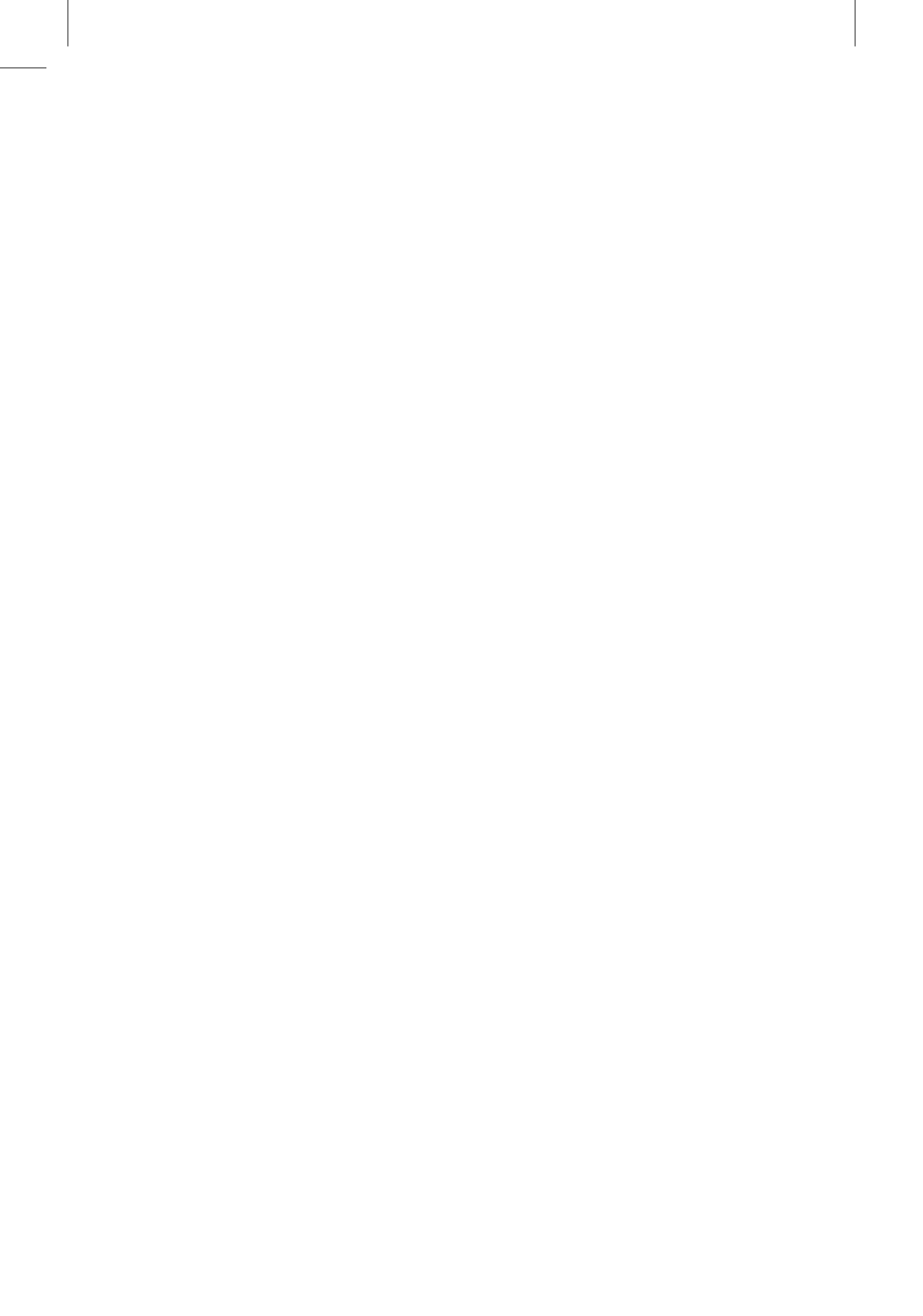
have been considered in their risk assessment? Have they looked at the  
(2)-6(vi1-3799emplendo)(ty68646)5d71(686801)268:54manag8786(2)and17991101at64-66734(1c)1302d9(Tthp22

This requires the third-party vendor to disclose not only its breach history regarding regulated data, but also, if specified, any security incidents or breaches involving intellectual property and trade secrets. Making a decision about a third-party vendor, if it is to be handling any type of sensitive information, requires understanding its threat environment and the risk potential. Arriving at a decision about its suitability to

determining how the company audits itself, what it is able to detect and prevent, and what it has not been successful in detecting and preventing. Additionally, require the third party to accept a provision in the service









up on site, vendors may get the idea that you aren't taking the breach seriously—

de nition of the cyber attack and resulting losses. The greater the  
de nition of the required documentationrvendod the5ile

5vre

ee

theendr533(oe)33(rn)-497.8esuldn

tncluden theol

r(eq

IBM indicated that 77 percent of respondents were concerned that cloud computing would increase privacy risk.











crew back home alive. But thanks to the mission control team at NASA and the grit of the *Apollo* 13 astronauts, Apollo was a successful failure—the







## THE GOAL OF THE EXECUTIVE CYBER RISK COUNCIL

council react? What would be their function? How would they work together? What would they tell employees? What would they say to the media and to business partners? How would they stop the breach? How would they investigate it? Who should contact law enforcement? Which law enforcement agency should be contacted, and when? What about getting the regulators involved? Which ones? When?

An effective executive cyber risk council can address these and other questions before a strike occurs, helping to reduce the impact of a potentially devastating cyber attack, and maintain that ever important bond of trust,

advice and counsel, resulting in a better conclusion to the case. The company did not have the satisfaction of seeing the justice system work to its maximum potential, and the criminal is likely working elsewhere, perpetrating another fraud. So getting the right legal counsel can have a major impact.

Placing a knowledgeable and experienced attorney with privacy, data protection, and law enforcement experience on the team can be invaluable.

Risk of cer. Some companies have a chief risk7(c)-1xf3.1(a)-rif8712.145m.5gD(cer.)Tj/F.5









Alliance management. Strategic alliance and joint venture partner

Independent adviser. An outside opinion is always advisable. Bringing in an independent third party has the advantage of providing a perspective that is not influenced by corporate politics or trying to impress the boss with showboating. An independent adviser can contribute information and

cyber complications springing from the cyber threat is through the executive cyber risk council. Every member has a voice. Every member has a perspective—and a responsibility. And every member has a vested interest in the outcome. The problem is vastly more complex than any Ce.Andis41430.1(the4)-174solucatin(in)50





It is no secret that some of the better-protected companies are those that have felt the pain of a prior breach. Depending on a number of conditions associated with the company and its attackers, that pain may have been signi













breach in your company, there is a better than reasonable likelihood that the breach will come via a third-party vendor.

Here's another tip. Monitor what employees are actually doing, especially those with access to sensitive data. Web surfing is often monitored, for example.











# About Author7







establishing attorney-client privilege, 132

Sherwood, Robert E., 101  
Singapore, 27