What Can Go Wrong: Telecom

1. Management did not invoice a related party customer for several T1 and DS3 special circuits, so the subsidiary's earnings would look more attractive to potential investors. Over the course of two years, $1.7 million in expenses were kept off the subsidiary's bottom line.
2. A collector provided numerous friends and family members with free phone service by crediting their balance dues every month.
3. A private technology company distributed software and hardware tools allowing customers to modify their modems so they could disguise themselves as paying customers and obtain internet service without paying.
4. The director of international relations doled out business to foreign telecom companies in exchange for bribes paid into two shell companies owned by him.
5. The cashier supervisor collected all walk-in customers' payments at the end of every day, set aside the checks, and took the cash to a casino. She planned to return the cash and just keep the gambling winnings.
6. Sales personnel switched customers' service without the customer's authorization. In some instances, the salesperson forged the customer's signature on a service transfer form.
7. The CFO directed line cost expenses to be capitalized and then depreciated. Over $6 billion in expenses were capitalized over several years.
8. In order to conceal irregularities from the auditors, accounting booked top-side entries to smooth accounts, thereby avoiding the auditors' scope for testing accounts.
9. A customer applied for cell phone service using a false name and address. Instead of paying their monthly bill, they re-applied for service with a new name and address.
10. A customer acquired phone service using the stolen identity of a person known to have good credit. The customer called a customer service rep, impersonating the person whose identity they stole, and explained to the CSR that they just changed addresses and required service at the new address.
11. A fraudulent user gained access to the VOIP network and acquired a list of unique phone numbers the network managed. The user then sold those phone numbers and access.
12. Billing added a nominal amount, such as 0.99 or 1.99, to every customer phone bill as a 'service fee' or some other innocuous description the customer was unlikely to notice, yet no service was being provided to the customer for that fee.

13. The IT director, in charge of procuring high-dollar network hardware, obtained the hardware from a legitimate vendor and had it shipped to the proper location. However, the director asked the vendor to invoice a shell company he had created. He marked up the invoices, then had the shell company invoice his employer, and he approved those invoices. He collected $5 million on the mark-ups.
14. A salesperson called commercial customers and explained their analog phone system had become obsolete, and told the customer if they signed a new lease they would receive cash back, thus in effect a free system upgrade. The telecom provider had no such cash-back deal, and the salesperson received cash up-front because they would sell the lease to a third-party contract administrator.
15. In a scheme known as a “bust-out,” the customer, having established some credit with the telecom company, purchased ever-increasing blocks of phone-line capacity, then resold the capacity. Then, the customer would not pay the telecom supplier for the final, largest blocks acquired.
16. Intruders gain access to businesses that use a PBX phone/voicemail system and use system commands such as an 800 number or other access number to gain a dial tone. They place unlimited long-distance calls directly through these lines for unscrupulous operators reselling long-distance at a profit.
17. A foreign user with a counterfeit cell phone is able to clone the electronic serial number and telephone number of a subscriber’s phone, and gains access to the network through a legitimate customer. The user makes long-distance phone calls to their home country through the legitimate user’s line, and thus the real subscriber gets billed for the calls.
18. An outside user impersonated an installer or colluded with an inside employee to be transferred to "9-0" or some other outside toll number (9 providing access to an outside line and 0 connecting to the utility's operator). The call appeared to originate from the business and therefore landed on the company's phone bill.
19. A regional service provider with access to the central office and the assignment system received kickbacks from the customer to provision special circuits to the customer, yet never posted an order nor inform billing. Because the order, assignment, and billing systems were all separate, no one else was alerted to the problem.
20. Service drivers used fleet vehicles for personal trips, and used company-paid fuel cards to fill up their personal vehicles.
21. A service employee ran a side business using the company truck and parts, and occasionally performed new installations without the company’s knowledge because the customers were willing to pay cash to have the employee come to the house on a weekend for a discount.

22. During a residential service call, the technician intentionally damaged customer's property in order for the customer to require they return on a weekend and pay cash for the repair.
23. Warehouse employees stole cable and sold it to recyclers.
24. Employees stole new product offerings such as the latest cell phone models and sold them in online auctions.
25. A cable vendor regularly shorted the length of cable on the spool by several meters. Because the spools contained over a thousand meters of cable, no one noticed the shortage.
26. Excess material was always delivered to an installation job. However, the excess was never returned to the yard; installers and contractors arranged to have it sold as scrap.
27. An employee with access to the billing system downgraded the service billing tariff for friends and family members.